

US/CA et al., ex rel. SEALED

v.

SEALED

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA, THE)
STATES OF CALIFORNIA,)
DELAWARE, FLORIDA, HAWAII,)
ILLINOIS, INDIANA, IOWA,)
MASSACHUSETTS, MINNESOTA,)
MONTANA, NEVADA, NEW JERSEY,)
NEW MEXICO, NEW YORK, NORTH)
CAROLINA, RHODE ISLAND,)
TENNESSEE, VERMONT, and)
VIRGINIA, and THE DISTRICT OF)
COLUMBIA and NEW YORK CITY)
ex rel. JOSHUA M. BOYCE

Civil Action No. _____

**FILED IN CAMERA
AND UNDER SEAL**

Jury Trial Requested

Plaintiff-Relator

v.

SALESFORCE, INC.

Defendant.

COMPLAINT

Table of Contents

I.	STATEMENT OF THE CASE	1
II.	LEGAL FRAMEWORK	11
A.	Parties	11
B.	Jurisdiction and Venue	13
C.	Time Period	13
D.	The Laws Violated	14
1.	Federal False Claims Act	14
2.	State/Local False Claims Acts	16
III.	BACKGROUND	16
A.	Government Cybersecurity Requirements	17
1.	Identify	31
2.	Protect	32
3.	Detect	36
4.	Respond.....	37
5.	Recover	39
B.	Salesforce	40
1.	GovCloud: Zero Trust Environment.....	41
2.	Platforms/Products	44
3.	Cyber Response.....	47
C.	The Government Contracts	54
1.	Federal Contracts	56
2.	State/Local Contracts	59
IV.	THE FRAUD SCHEME.....	64
A.	Knowingly Exposing Government and Consumer Data to Possible Malicious Actors	70
1.	Knowingly Enabling Cloaked Attacks.....	71
a.	Tableau Platform	72
(i)	Cyber Incident #1	74
(ii)	Cyber Incident #2.....	77

(iii)	Cyber Incident #3.....	78
b.	MuleSoft Platform	80
(i)	Cyber Incident #4.....	81
(ii)	Cyber Incident #5.....	83
2.	Knowingly Enabling Conspicuous Attacks	85
a.	Cyber Incident #6	86
b.	Cyber Incident #7	89
c.	Cyber Incident #8	91
B.	Knowingly Exposing Government and Consumer Data to Actual Breaches	92
1.	Cyber Incident #9.....	94
a.	Cyber Incident #10	95
b.	Cyber Incident #11	97
c.	Cyber Incident #12	98
d.	POLARIS.....	101
2.	Cyber Incident #13.....	103
3.	Codecov	107
C.	Knowingly Perpetuating Imminent Threats to Government and Consumer Data	111
V.	MATERIALITY	122
VI.	UNLAWFUL RETALIATION	130
VII.	COUNTS	132

This is a False Claims Act *qui tam* action by Relator to recover treble damages and civil penalties arising from the actions of Salesforce Inc. (“Salesforce”).

I. STATEMENT OF THE CASE

1. Salesforce, Inc. is a publicly traded American cloud-based software company with international operations with over 73,000 employees and 110 offices worldwide. It provides customer relationship management software and applications focused on sales, customer service, marketing automation, analytics, and application development. Salesforce boasts that “over 150,000 companies, both big and small, are growing their businesses with Salesforce...” “[t]he World’s #1 CRM [customer relationship management] platform.” Internal documents show that number is as high as 250,000, many of which are federal, state and local government agencies.

2. Government agencies contract with Salesforce to provide them with cloud services and computing and software platforms to support their operations. Agencies also run businesses and health care operations no different than private companies and providers. So, for example, the U.S. Department of Veterans Affairs contracts with Salesforce to help it administer health care to veterans. The VA trusts that the Salesforce platform is securely storing the HIPAA-protected medical records of veterans.

3. As part of its contracts with Salesforce, the U.S. Department of Defense (DOD) and its sub-agencies like the National Security Division contract with Salesforce to facilitate military and national security operations. DOD trusts that Salesforce is securely handling this sensitive data.

4. The U.S. Department of Health and Human Services (DHHS) contracts with Salesforce for COVID-19 tracing and vaccine management, and the Commonwealth of Massachusetts contracts with Salesforce to manage vaccine recipients and their household members, creating an immunization registry and using a Salesforce platform “to move data from the immunization registry to the State’s system.” DHHS and the Commonwealth of Massachusetts trust that Salesforce is securely handling HIPPA-protected patient information.

5. Federal, state and local government agencies have paid Salesforce billions of dollars to help manage, process, and confidentially store large volumes of sensitive government data at all levels of sensitivity, including classified information.

6. Salesforce offers a cloud service known as “Government Cloud” or “GovCloud,” specifically for use by government agencies and government contractors. Salesforce represents that GovCloud is “a unique, limited access Salesforce environment that is configured differently than other production environments to meet stricter security requirements” to store sensitive government

data. Salesforce also represents that GovCloud is a “Zero Trust Environment” meaning that anyone—including any of the over 73,000 Salesforce employees—is a possible malicious actor. Access to GovCloud is required to be limited to individuals who have undergone special security processes and background checks, so, it is a violation of Government Cybersecurity Requirements to allow unauthorized individuals to access GovCloud. With that in mind, Salesforce represents that all GovCloud users are authenticated, validated, and authorized before gaining access to any application or data in GovCloud. Unauthorized access to sensitive government data jeopardizes national security, government programs and consumer protection, and the confidentiality of the sensitive data.

7. Salesforce further represents that “[c]ompliance and vulnerability reporting in [GovCloud] is far more robust and more scrutinized than any other environment; it is the most secure environment at Salesforce. Data in [GovCloud] is strictly kept in [GovCloud], and many [Salesforce] teams have no personnel with [GovCloud] access.”

8. Like any private company, the government expects that it will get what it paid for. In this case, the government expected Salesforce to provide it cloud services and computing software platforms that were secure—i.e., that Salesforce was taking defensive cyber measures to reduce the risks of intrusions, attacks, and the effects of natural or manmade disasters on critical infrastructure.

9. However, the government did not get what it paid for.

10. Salesforce's federal government contracts are subject to the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS) for contracts with DOD, and other agency-specific regulations and standards issued by the Federal Risk and Authorization Management Program (FedRAMP) and the National Institute of Standards and Technology (NIST)—the federal agency that establishes standards and best practices for several industries. Salesforce's state and local government contracts are subject to similar requirements. These independent and overlapping "Government Cybersecurity Requirements" create a robust and comprehensive regulatory environment.

11. Salesforce has numerous written policies to implement these Government Cybersecurity Requirements. However, while Salesforce compliance looks good "on paper," it has routinely violated these requirements, including its own written policies.

12. At times, government employee login credentials (usernames, passwords, tokens, and keys) were leaked on the internet. This allowed possible malicious actors cloaked as government employees to obtain access to sensitive data. At other times, the attacks were more conspicuous but no less harmful to the government. Attacks on GovCloud were enabled through Salesforce-owned

platforms such as Tableau, MuleSoft and Heroku. Sometimes, known vulnerabilities may or may not have led to actual breaches of government data. Yet Salesforce knowingly and routinely failed to act in response to known vulnerabilities.

13. And known data breaches did occur. One such cyber incident codenamed Cyber Incident #12 led to the breach of GovCloud data of 13 or more agencies with dozens more made vulnerable and impacting thousands of government employees in July 2020. In another instance, in March 2022, government data was “spilled” into unsecure cloud environments over 32 million times, directly impacting at least 100 government agencies. According to internal Salesforce documents, “any customer who sent an email in last nine days would be impacted so it should be most of the customers.” Salesforce routinely discovered cybersecurity vulnerabilities and data leaks by pure happenstance instead of through robust cybersecurity measures; most of the examples of cyber incidents in this Complaint were discovered this way. And Salesforce routinely failed to properly respond when cybersecurity violations were discovered.

14. Salesforce’s failure to remedy one serious cyber incident caused other serious cyber incidents, creating a domino effect. Its routine failure to take affirmative steps to remedy cyber incidents had the effect of a disastrous oil spill.

Failure to clean up the first oil spill created a bigger challenge to contain and control the later oil spills.

15. Further, there is imminent threat from Salesforce's continuing violations of Government Cybersecurity Requirements. One recent disaster involved Salesforce's reckless use of the Zoom platform. This time last year, Salesforce customers including government users experienced a massive outage. Concerned solely about its business image, Salesforce pushed out an informational webinar on Zoom to 50,000 affected users to mollify them. In doing so, it dispensed with authentication requirements and allowed widespread credentials-sharing among employees making possible malicious actors anonymous. This triggered a self-inflicted cyber threat. Salesforce's intentional disregard for government rules paved the way for possible malicious actors to launch attacks on the government and learn more about GovCloud's vulnerabilities through cloaked participation in these Zoom webinars. Essentially, Salesforce enabled malicious actors to be a fly on the wall during these webinars. Prioritizing expediency over cybersecurity, Salesforce violated Government Cybersecurity Requirements and its own written protocols.

16. Salesforce's violations ran the gamut from unaddressed software engineering failures that knowingly put government data at risk (e.g., Cyber Incident #6) to intentional whitewashing of known vulnerabilities (e.g., the Zoom

cyber threat). It encompassed all its products, among them GovCloud, Tableau, MuleSoft, Heroku.

17. All kinds of sensitive data with varying degrees of sensitivity were breached or made vulnerable to breach on Salesforce's watch:

- data about government agencies, operations, logistics
- internal government agency communications
- government employees' PII and login credentials (usernames, passwords, tokens, and keys)
- the data of non-governmental businesses and private consumers such as patients, U.S. military members and veterans who are the beneficiaries of certain government contracts with Salesforce
- detailed histories showing the activities of government employees on GovCloud, such as data accessed, reviewed, revised, shared (when and with whom)
- the names (or titles) and locations of government data, including documents, spreadsheets, presentations, memos, and other information stored on GovCloud
- details of government agency cyber vulnerabilities

18. Salesforce's motivation in giving short shrift to cybersecurity protections can be explained by expediency over safety, with Salesforce bragging that customers experience "29% *faster*-decision making, 30% *faster* collaboration, 30% *faster* response time, and 29% *faster* resolution time." (emphasis added)

19. In today's cloud-based environment, the government naturally expects that their contractors will routinely experience cyber threats. Yet government agencies have relied to their detriment upon Salesforce's representations that it will identify, protect against, detect, respond to and recover from cyber incidents involving sensitive government data. The allegations in this Complaint do not hold Salesforce accountable for risks posed by malicious actors, but rather for its knowing and routine failure to take all the steps that are necessary and required to identify, protect against, detect, respond to, and recover from cyber incidents. It is not the existence of malicious or possible malicious actors, but the consistent failure to properly respond to known vulnerabilities and the failure to properly disclose these vulnerabilities to the government that gives rise to Salesforce's False Claims Act liability.

Government agencies that contract with Salesforce are sitting ducks left vulnerable to malicious actors.

20. Because of persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent

claims to government agencies and submitted false records material to fraudulent claims, and the government agencies paid those claims. This case is precisely the type of fraud scheme the U.S. Department of Justice is seeking to remedy under the False Claims Act.

21. The Deputy Attorney General (DAG) announced in October 2021 that DOJ created a Civil Cyber-Fraud Initiative to pursue cyber fraud by government contractors like the fraud scheme alleged here, to “hold accountable entities or individuals that put U.S. information or systems at risk by

- knowingly providing deficient cybersecurity products or services
- knowingly misrepresenting their cybersecurity practices or protocols, or
- knowingly violating obligations to monitor and report cybersecurity incidents and breaches.”

“[P]rotecting against malicious cyber campaigns is a matter of national concern and a top priority for the [current] Administration.” Thus, “[w]hen companies that do business with the government knowingly make misrepresentations about their own cybersecurity practices, or when they fail to abide by cybersecurity requirements in their contracts, grants or licenses, the government does not get what it bargained for.” And “when false assurances are made to the government,

sensitive government information and Systems may be put at risk without the government even knowing it.” Press Release, Office of Public Affairs, U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>; and Remarks of Brian Boynton, Acting Assistant Attorney General, Civil Division, U.S. Department of Justice (Oct. 13, 2021), <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

22. Use of the False Claims Act as an enforcement tool in this case will hold Salesforce accountable for its knowing and material violations of Government Cybersecurity Requirements, deter imminent threats caused by Salesforce and other government contractors, and protect sensitive government data from exposure in the event of an attack on Salesforce systems like (or worse than) the SolarWinds Attack two years ago.

23. The DAG further directed comments at whistleblowers: “to those who witness irresponsibility that exposes the government to cyber breaches, our message is this: if you see something, say something.” But for Relator the government would not be on notice of the allegations in this Complaint. Remarks of Lisa O. Monaco, Deputy Attorney General, U.S. Department of Justice (Oct. 20,

2021), <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr>

II. LEGAL FRAMEWORK

A. Parties

24. Relator alleges, based upon personal knowledge, relevant documents, and information, and on information and belief, the facts set forth in this Complaint.

25. Relator has extensive first-hand knowledge of Defendant's pattern and practice alleged in the Complaint.

26. Relator was retaliated against for raising, objecting to, and opposing fraudulent conduct alleged in this Complaint.

27. Relator has standing to bring this action pursuant to 31 U.S.C. § 3730(b)(1). Relator is entitled to either between 15-25 percent of the proceeds that result from this action, or any settlement of the claims raised or identified in this complaint, under [31 U.S.C. § 3730\(d\)\(1\)](#); or between 25-35 percent of the proceeds pursuant to [31 U.S.C. § 3730\(d\)\(2\)](#); or of any amounts specified in any state's False Claims Act.

28. Pursuant to subsection (e)(4)(A) of [31 U.S.C. § 3730](#), Relator voluntarily disclosed to the government the information on which the allegations or transactions in the claims are based; and Relator has knowledge that is independent

of and materially adds to any publicly disclosed allegations or transactions that may exist and has voluntarily provided the information to the government before filing an action under this section. 31 U.S.C. § 3730(e)(4)(A). Relator is the original source of these allegations as defined in 31 U.S.C. § 3730(e)(4)(B).

29. Relator has complied with all procedural requirements of the laws under which this Complaint is brought.

30. Defendant Salesforce, Inc. is an American publicly traded, international Cloud computing Enterprise software company with over 73,000 employees and 110 offices worldwide. It is incorporated in Delaware, with Worldwide Corporate Headquarters in San Francisco, California.

31. Salesforce also has an established presence in Greater Boston since 2014, with a Corporate Office at 500 Boylston in Boston, Massachusetts, and Offices in Burlington and Cambridge, Massachusetts, with 1,450 employees in Greater Boston. According to its website, “Salesforce, the global leader in customer relationship management (CRM), has a presence throughout the *Greater Boston area*. Leading with our values — trust, customer success, innovation, and equality — has been critical to our success. *Our proximity to some of the country's leading higher education and healthcare companies has helped fuel our local economy and accelerate our growth in key industries, as well as across the business.*” (emphasis added)

32. Salesforce provides customer relationship management software and applications focused on sales, customer service, marketing automation, analytics, and application development. It was founded in 1999 and has over 250,000 customers, including thousands of federal, state, and local government agency customers.

B. Jurisdiction and Venue

33. This Court has subject matter jurisdiction over the claims asserted in this Complaint, pursuant to the False Claims Act, 31 U.S.C. §§ 3729 et seq., including § 3730(h), and 28 U.S.C. §§ 1331, 1345. This Court also has supplemental jurisdiction over the related state law claims pursuant to 28 U.S.C. § 1367(a).

34. Venue is proper in this judicial district, pursuant to 31 U.S.C. §§ 3732(a) and 28 U.S.C. 1391(b) and (c), because defendant may be found, resides, and/or transacts business in this District, or because an act, proscribed by 31 U.S.C. § 3729, occurred in this District.

C. Time Period

35. On information and belief, Defendant's fraudulent conduct alleged in this Complaint began at least as early as 2015.

D. The Laws Violated

1. Federal False Claims Act

36. This Complaint alleges violations of the Federal False Claims Act. The False Claims Act provides that any person is liable to the United States for a civil penalty, which is adjusted by the Federal Civil Penalties Inflation Adjustment Act of 1990, plus three times the amount of damages which the government sustains because of the act of that person, if the person commits any of these violations:

(A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval

(B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim

(C) conspires to commit a violation of subparagraph (A), (B), or (G) of the False Claims Act,

(G) knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the government.

31 U.S.C. § 3729(a)(1)(A), (B), (C), (G).

37. Under the False Claims Act, scienter must be demonstrated, by showing the alleged conduct was “knowing” or done “knowingly,” which means that (A) a person, with respect to information— (i) has actual knowledge of the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information; and (B) require no proof of specific intent to defraud. 31 U.S.C. § 3729(b)(1).

38. Further, the term “claim ” means any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that— (i) is presented to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the government’s behalf or to advance a government program or interest, and if the United States Government— (I) provides or has provided any portion of the money or property requested or demanded; or (II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded; []. 31 U.S.C. § 3729(b)(2).

39. Under the False Claims Act, materiality is defined as “having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.” 31 U.S.C. § 3729(b)(4).

2. State/Local False Claims Acts

40. The False Claims Act of numerous states and cities are alleged in this Complaint, including the States of California, Delaware, Florida, Hawaii, Illinois, Indiana, Iowa, Massachusetts, Minnesota, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, Rhode Island, Tennessee, Vermont, and Virginia, the District of Columbia, and New York City.

III. BACKGROUND

41. Salesforce must adhere to numerous government cybersecurity requirements that mandate Salesforce (a) Identify; (b) Protect; (c) Detect; (d) Respond; and (e) Recover when securing its information systems and addressing cyber threats, including threats to Salesforce's government cloud environment and its cloud products, among them Tableau, MuleSoft, and Heroku. With customers that include hundreds of federal, state and local government agencies with collective contracts worth billions, Salesforce plays an essential role in safeguarding national security and government programs and consumer protection by ensuring Salesforce adequately protects the "data and information" transferred under those contracts. (Data and information are used interchangeably throughout this Complaint and are intended to have the broadest possible meaning; and data and information refers to both the government's data as well as consumer data, i.e., the customers and beneficiaries of the government contracts.)

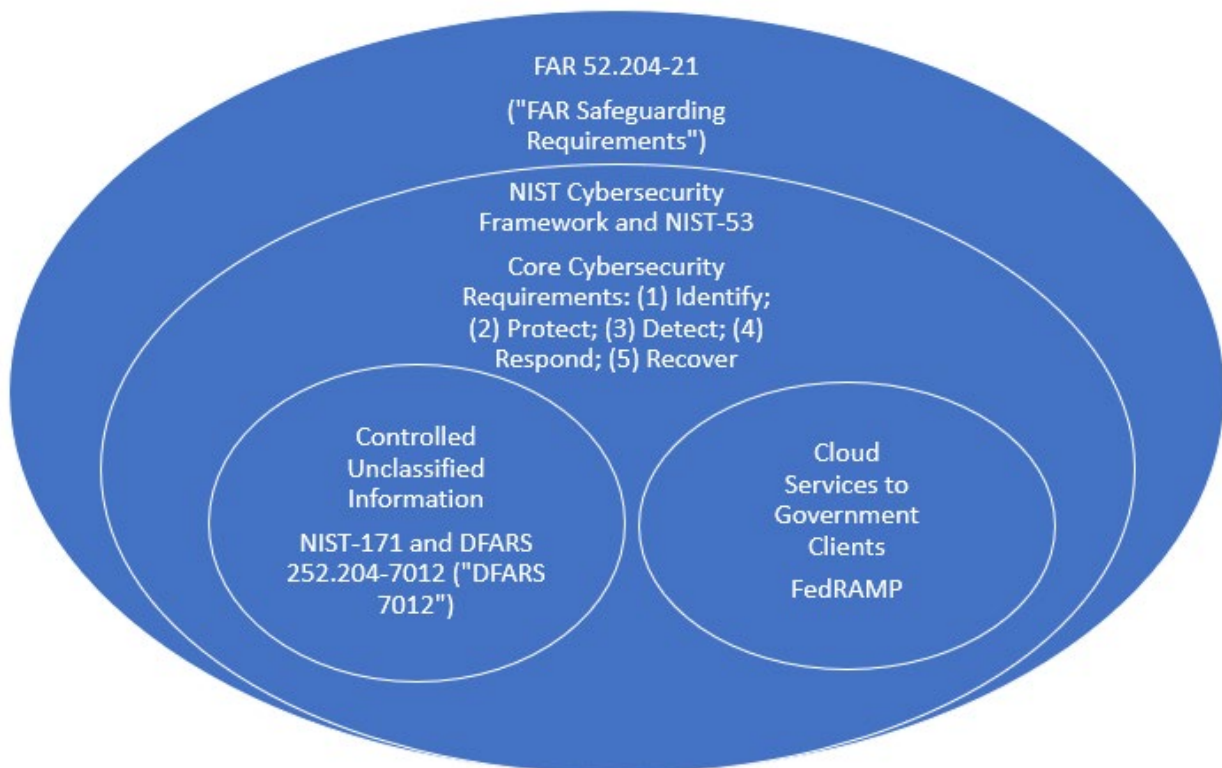
A. Government Cybersecurity Requirements

42. Federal government contracts like those at issue in this case are subject to the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS) for contracts with DOD, and other agency-specific regulations and standards issued by the Federal Risk and Authorization Management Program (FedRAMP) and the National Institute of Standards and Technology (NIST)—the federal agency that establishes standards and best practices for several industries. Salesforce’s state and local government contracts are subject to similar requirements. These independent and overlapping requirements often reiterate, build upon and further specify preexisting cybersecurity requirements to create a robust and comprehensive regulatory environment. These same or similar requirements are also imposed by state and local government agencies under their contracts with Salesforce.

43. Collectively, the government contracting requirements at issue in this Complaint and set forth under this Section are alleged as “Government Cybersecurity Requirements.” 48 C.F.R. § 52.204-21 (2021) (“FAR Safeguarding Requirements”); 48 C.F.R. § 252.204-7012 (“DFARS 7012”); NIST-53, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>; NIST-61, <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>, NIST-92, <https://csrc.nist.gov/publications/detail/sp/800-92/final>, NIST-171,

<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>; NIST Cybersecurity Framework, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>; FedRAMP, <https://www.fedramp.gov/>

44. This Venn diagram demonstrates the overlapping Government Cybersecurity Requirements for a contractor like Salesforce:



45. The NIST Cybersecurity Framework forms a baseline against which to measure a government contractor's efforts to secure a network that houses sensitive government data. From there, contractors are subject to even more stringent cybersecurity requirements. NIST Cybersecurity Framework, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

46. The FAR sets minimum security requirements for all federal contractors to “protect” their information systems—for example, host servers, workstations, routers and the cloud environment—that process, store, or transmit government data which is not intended for public release under a federal contract. 48 C.F.R. § 52.204-21(a), (b)(1) (FAR Safeguarding Requirements); 81 Fed. Reg. 30439, at 30441 (2016)

47. The FAR is clear that these cybersecurity protections are intended for the “information system as a whole, rather than just the protection of the [f]ederal contract information,” imposing on contractors the requirement to safeguard their whole information system because cyber threats can manifest internally, as well as externally. 48 C.F.R. § 52.204-21(b)(1) (FAR Safeguarding Requirements); 81 Fed. Reg. 30439, at 30443 (2016)

48. “Federal contract information” is further defined as “information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government” 48 C.F.R. § 52.204-21(a) (FAR Safeguarding Requirements); 81 Fed. Reg. 30439, at 30441 (2016)

49. At this baseline, federal contractors must implement fifteen “basic” security controls to protect the information systems that process, store, or transmit federal contract information. Because these requirements apply to the information

system itself, they do not vary based on the type of non-public government data at issue: “The rule makes clear that [f]ederal contractors whose information systems process, store, or transmit [f]ederal contract information must follow these basic safeguarding standards.” [48 C.F.R. § 52.204-21\(b\)\(1\)](#) (FAR Safeguarding Requirements); [81 Fed. Reg. 30439](#), at 30440-30442 (2016)

50. The FAR Safeguarding Requirements, like other Government Cybersecurity Requirements, reiterate and reinforce the application of “[NIST] information systems requirements to contractors and, by doing so, help to create greater consistency, where appropriate, in safeguarding practices across agencies.” *See, e.g.,* [81 Fed. Reg. 30439](#) at 30440, 30442 (2016)

51. NIST promulgates foundational cybersecurity requirements under Executive Orders and in furtherance of its statutory responsibilities under the Federal Information Security Modernization Act (FISMA). These NIST standards are essential because of the growing recognition that cybersecurity can impact critical infrastructure and the stored sensitive government data. [44 U.S.C. § 3551](#) *et seq.*, Public Law (P.L.) 113-283.

52. In a February 12, 2013, Executive Order titled “Improving Critical Infrastructure Cybersecurity,” President Barack Obama noted that:

Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The

cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.

Critical infrastructure means “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>, §§ 1-2

53. Under this Executive Order, President Obama directed the development “of a framework to reduce cyber risks to critical infrastructure.” So, the NIST Cybersecurity Framework was first promulgated in February 2014 to “include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.” It was updated on April 16, 2018. (Except where otherwise noted, this Complaint refers to the 2018 version of the NIST Cybersecurity Framework, and references to the NIST standards are intended to incorporate historical and current versions of those

standards.) <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>,

§ 7; NIST Cybersecurity Framework,

<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

54. The core requirements provide concrete actions to be taken by government contractors to mitigate harm from the risk of cyber threats:

NIST Cybersecurity Framework	Required Cybersecurity Actions
Identify	<ul style="list-style-type: none"> • Inventory • Understand cybersecurity risks • Comply with Government cybersecurity alerts
Protect	<ul style="list-style-type: none"> • Employ identity management and access controls (e.g., usernames, passwords, authentication) • Ensure boundary protections to mitigate against data leaks and spills
Detect	<ul style="list-style-type: none"> • Monitor system • Analyze logs to determine anomalous activity
Respond	<ul style="list-style-type: none"> • Analyze logs to understand impact • Rapid detection and rapid response

	<ul style="list-style-type: none"> • Report cybersecurity incidents consistent with established policies
Recover	<ul style="list-style-type: none"> • Incorporate lessons learned

55. Following onto the 2013 Obama Executive Order, on May 12, 2021, President Biden signed Executive Order 14028 called “Improving the Nation’s Cybersecurity,” and declared that “the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.” This statement of policy was supported by his determination that the country “faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy.” Moreover, President Biden observed that to secure the nation’s sensitive information from compromise, “[t]he private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.”

<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>, § 1

56. The 2021 Biden Executive Order went beyond mandating general cybersecurity protections and discussed specific requirements for government contractors including:

- “advance toward Zero Trust Architecture;”
- “accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS);”
- “centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks;” and
- “invest in both technology and personnel to match these modernization goals.”

<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>,

§ 3(a)

57. Federal contractors are expected to ensure the provision, maintenance, and oversight of at least the five cybersecurity core requirements through referenced and incorporated security and privacy controls, including from NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations* (“NIST-53”). NIST-53 provides a “a comprehensive set of security and privacy safeguarding measures for all types of computing

platforms, including general purpose computing systems, cyber-physical systems, cloud systems, mobile systems, industrial control systems, and Internet of Things (IoT) devices.” NIST Cybersecurity Framework, at p. 6-7, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>; NIST-53 at ix, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

58. Further, a contractor has heightened cybersecurity obligations with regards to a subset of sensitive government data called Controlled Unclassified Information (“CUI”). “The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions.” Thus, “[s]ystems that contain classified information, or CUI such as personally identifiable information, require more than the basic level of protection.” NIST-171 at iii, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>; 89 Fed. Reg. 30439, at 30439 (2016)

59. CUI is unclassified information that is intended to be non-public because of the sensitive nature of the information, such as personally identifying information. CUI includes information marked FOR OFFICIAL USE ONLY (“FOUO”) and NOT RELEASABLE TO FOREIGN NATIONALS (“NOFORN”). <https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive->

[order-13556-controlled-unclassified-information](#); [81 Fed. Reg. 30439](#), at 30439, 30442 (2016)

60. NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (“NIST-171”) establishes 110 baseline security standards for federal contractors that process, store, or transmit CUI. The NIST-171 security requirements fall into the following categories, or families, of controls:

TABLE 1: SECURITY REQUIREMENT FAMILIES	
FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

NIST 800-171 at 7, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

61. “The requirements [of NIST-171] apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.” NIST-171 at p. iii, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

62. The controls in NIST-171 derive from, and provide greater specificity to, the controls in NIST-53, and are focused on protecting the confidentiality of CUI. Revisions to NIST-171 are tied to revisions in NIST-53.

https://www.nist.gov/system/files/documents/2018/10/18/cui18oct2018-104501145-dod_dfars-michetti-thomas.pdf, at p. 7, 15; NIST-171 at vi, 6, <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

63. A DOD cybersecurity rule requires defense contractors and subcontractors whose computer networks will house CUI during performance of a contract to comply with the controls of NIST-171 to “provide adequate security” on any such network. “Adequate security” is defined as “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.” [48 C.F.R. § 252.204-7012\(a\), \(b\)](#) (DFARS 7012); [78 Fed. Reg. 69273](#), at 69279 (Nov. 18, 2013); [48 C.F.R. § 204.7301](#); [48 C.F.R. § 204.7302\(a\)\(1\)](#)

64. Under this DOD cybersecurity rule, contractors and subcontractors must also immediately report cyber security incidents occurring on such networks (or any compromise of such networks) to DOD. Specifically, the contractors must “rapidly report,” directly to the appropriate agency officials, any cyber incident. Rapidly report means within 72 hours of discovery of any cyber incident. 48

C.F.R. § 252.204-7012(a), (c)(1)(ii) (DFARS 7012); 78 Fed. Reg. 69273 (Nov. 18, 2013); 48 C.F.R. § 204.7302(b)

65. DFARS 7012 also requires that contractors fully comply with the NIST-171 standards in effect at the time of the contract solicitation as soon as practicable, but not later than December 31, 2017. Although NIST-171 was further revised in February 2020 with minor technical edits, the security requirements are consistent between the 2 versions. 48 C.F.R. § 252.204-7012(b)(2)(i), (ii)(A) (DFARS 7012); 78 Fed. Reg. 69273 (Nov. 18, 2013); <https://www.nist.gov/news-events/news/2020/02/nist-publishes-sp-800-171-revision-2-protecting-controlled-unclassified>

66. Additionally, all DOD solicitations and contracts, task orders, and delivery orders, except for commercial off the shelf items, issued after November 30, 2020, require contractors to complete a self-assessment of their compliance with NIST-171. Contractors must also provide DOD access to the contractor's facilities, systems, and personnel as necessary for the government to complete its own assessment of the contractor's compliance with NIST-171. 48 C.F.R. § 252.204-7020

67. In June 2022, the DOD reaffirmed the critical nature of contractor compliance with NIST-171:

The protection of controlled unclassified information on contractor information systems is critically important to the Department of Defense (DOD). . . .

DFARS clause 252.204-7012 requires a contractor to implement, at minimum, the NIST SP 800-171 security requirements on covered contractor information systems.

Contractors must implement all of the NIST SP 800-171 requirements and have a plan of action and milestones (per NIST SP 800-171 Section 3.12.2) for each requirement not yet implemented. **Failure to have or to make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements.**

(emphasis added)

68. NIST-53 forms the baseline cybersecurity controls. NIST-171 requirements derive from the NIST-53 controls. The FAR Safeguarding Requirements then derive from and are consistent with NIST-171 controls. 81 Fed. Reg. 30439 at 30440 (2016)

69. Other government agencies also adopt NIST standards through the creation of complementary cybersecurity requirements. For example, contractors

that provide cloud services to government entities—like Salesforce—are known as “cloud service providers” and must satisfy certain cybersecurity requirements to receive certification from the Federal Risk and Authorization Management Program (“FedRAMP”). These FedRAMP security controls and enhancements are based on NIST-53 baseline controls.

70. FedRAMP serves as “a bridge between the federal government and industry” by providing “a standardized security framework for all cloud products and services that is recognized by all executive branch federal agencies.” FedRAMP was developed in collaboration with NIST and other government agencies to standardize how the Federal Information Security Management Act (FISMA) applies specifically to cloud computing services. Thus, to receive FedRAMP certification, a contractor must implement FedRAMP, i.e., NIST-53, security controls and enhancements within their cloud computing environment.

71. As a cloud service provider that contracts with Federal agencies, Salesforce had a contractual obligation to meet and maintain FedRAMP requirements and, by extension, the baseline controls in NIST-53.

72. Indeed, Salesforce represents itself and markets its various products as compliant with FedRAMP Moderate and FedRAMP High controls as well as all Government Cybersecurity Requirements.

73. Salesforce—an organization with access to large amounts of sensitive government data among them CUI and HIPAA-protected patient medical records through thousands of government contracts—understands its cybersecurity obligations and the necessity of complying with core requirements to (a) Identify, (b) Protect, (c) Detect, (d) Respond, and (e) Recover, relative to cybersecurity threats and vulnerabilities.

1. Identify

74. The Identify Function involves “[d]evelop[ing] an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.” These activities are “foundational” to the effective use of the rest of the NIST Cybersecurity Framework. NIST Cybersecurity Framework, at p. 7, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

75. Under the Identify Function, an organization is required to identify and manage the data, personnel, devices, systems, and facilities necessary to achieve its business purposes. As such, an organization is required to inventory physical devices, physical systems, software platforms, and applications within the organization. [48 C.F.R. § 52.204-21\(b\)\(1\)\(v\)](#) (FAR Safeguarding Requirements);

76. Additionally, an organization is required to understand the cybersecurity risk to organizational operations, assets, and individuals. This involves identifying and documenting asset vulnerabilities and both internal and

external threats. 48 C.F.R. § 52.204-21(b)(1)(xii) (FAR Safeguarding Requirements)

77. Thus, it is “essential” for organizations to comply with government security alerts, advisories, and directives about cybersecurity concerns “due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.”

NIST-53 at SI-5 Control and Discussion,

<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

2. Protect

78. The Protect Function involves “[d]evelop[ing] and implement[ing] appropriate safeguards to ensure delivery of critical services.” This Function is necessary to limit or contain the impact of a cybersecurity event. NIST Cybersecurity Framework, at p. 7,

<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

79. A cybersecurity event is a “cybersecurity change that *may* have an impact on organizational operations (including mission, capabilities, or reputation).” (emphasis added) NIST Cybersecurity Framework, at p. 45,

<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

80. Under the Protect Function, an organization is required to limit access to physical and logical assets to authorized users, processes and devices only. This involves issuing, managing, verifying, revoking, and auditing identities and credentials (usernames, passwords, tokens and keys) for authorized users, devices, and processes. 48 C.F.R. § 52.204-21(b)(1)(i), (ii), (iii) (FAR Safeguarding Requirements)

81. An organization is required to identify and authenticate each unique employee of the organization and be able to associate that employee with the processes taken on their behalf. Authentication means verifying a user's identity as a prerequisite to their accessing resources and information stored in an information system. To do this, an organization may employ passwords, physical authenticators, biometrics or, in the case of multi-factor authentication, some combination of these protections, to identify and authenticate users within the organization. 48 C.F.R. § 52.204-21(b)(1)(v), (vi) (FAR Safeguarding Requirement)

82. Additionally, only certain individuals within an organization should be given privileges. A "privilege is a special authorization that is granted to particular users to perform security relevant operations" such as authentication to access a system like GovCloud.

83. Routine authentication protocol for government users to access electronic systems and products using GovCloud, including usernames, passwords, tokens, or cryptographic key are called “secrets” under NIST, but more commonly known as credentials. The purpose of credentials to access electronic databases ensures that users can authenticate their identities and are authorized to have access to the appropriate electronic government data. “Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service.” NIST-63 at Introduction and § 4.3.1, <https://pages.nist.gov/800-63-3/sp800-63-3.html>

84. Further, an organization is required to implement and manage policies to respond to cyber threats. For example, an organization is required to have a plan in place to limit or contain the impacts of “spills” and “leaks” of information. “Information spillage” occurs when “information is placed on systems that are not authorized to process such information,” i.e., “when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level.” “Information leakage” is the “intentional or unintentional release of data or information to an untrusted environment from electromagnetic signals emanations.”

85. An organization is required to ensure data is secure by protecting the confidentiality, integrity, and availability of data-at-rest (e.g., user information) and data-in-transit. An organization is required to also implement protections against data or information leaks.

86. To ensure internal and external boundaries securely protect the data contained on any system, an organization is required to monitor and control communications at and within various managed interfaces, which “include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.” 48 C.F.R. § 52.204-21(b)(1)(x), (xiii), (xiv) (FAR Safeguarding Requirements); NIST-53 at SC-7 Control and Discussion, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>;

87. An organization is required to also use integrity checking mechanisms to verify software, firmware, information, and hardware integrity. Integrity checking involves verifying that the software, firmware, information, or hardware has not been altered without authorization.

88. And an organization is required to improve its protection processes as necessary to manage the protection of its information systems and assets that house sensitive government data.

3. Detect

89. The Detect Function involves “[d]evelop[ing] and implement[ing] appropriate activities to identify the occurrence of a cybersecurity event” in a timely manner. NIST Cybersecurity Framework, at p. 7, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

90. Under the Detect Function, an organization is required to detect anomalous activity and understand the potential impact of cybersecurity events. This detection involves collecting and correlating event data from multiple sources and determining the impact of an event. [48 C.F.R. § 52.204-21\(b\)\(1\)\(xii\), \(xv\)](#) (FAR Safeguarding Requirements)

91. Additionally, an organization is required to monitor for cybersecurity events and the effectiveness of protective measures, including through monitoring for unauthorized personnel, connections, devices, and software.

92. An important tool in an organization’s toolbox to monitor for anomalous activity and to analyze the impact of such activity is “logging.” A log is a record of events that occur within an organization’s systems and networks, such as audit logs tracking user authentication attempts and security device logs recording possible attacks. While NIST-53 includes several controls related to log management (such as controls for the generation, review, protection, and retention of audit records), NIST also promulgates Special Publication (SP) 800-92 (“NIST-

92”), which “provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization.” NIST-92 at 1-1, 2-1, 2-1 n.2, & 2-7, <https://csrc.nist.gov/publications/detail/sp/800-92/final>

4. Respond

93. The Respond Function involves “[d]evelop[ing] and implement[ing] appropriate activities to take action regarding a detected cybersecurity incident” to contain the impact. NIST Cybersecurity Framework, at p. 8, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

94. A cybersecurity incident is a “cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.” NIST Cybersecurity Framework, at p. 45, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

95. Under the Respond Function, an organization is required to report incidents consistent with established criteria and coordinate with internal and external stakeholders. [48 C.F.R. § 52.204-21\(b\)\(1\)\(xii\)](#) (FAR Safeguarding Requirements)

96. Additionally, an organization is required to conduct analyses to ensure effective responses and to support recovery activities. This analysis involves performing forensics and understanding the impact of the incident. An organization must then perform activities to contain and mitigate an incident.

97. NIST also promulgates a separate Special Publication, NIST SP 800-61 (“NIST-61”) to further explain an organization’s obligations to respond to a computer security incident. Incident response capability is “necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. To that end, this publication [NIST-61] provides guidelines for incident handling, particularly for analyzing incident related data and determining the appropriate response to each incident.” NIST-61 at p. 1, <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

98. NIST-61 further reinforces the need to properly analyze logs and understand the impact of a cyber threat, in order to respond accordingly: “In an organization, millions of possible signs of incidents may occur each day, recorded mainly by logging and computer security software. . . . Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.” NIST-61 at p. 3, <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

5. Recover

99. Lastly, the Recover Function involves “[d]evelop[ing] and implement[ing] appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.”

This Function supports “timely recovery to normal operations to reduce the impact from a cybersecurity incident.” NIST Cybersecurity Framework, at p. 8,

<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>

100. Under the Recover Function, an organization is required to improve recovery planning and processes by incorporating lessons learned into future activities and updating recovery strategies.

101. For example, NIST-53’s Incident Handling control recognizes that organizations should “[i]ncorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.” NIST also advises organizations to “[e]nsure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.” NIST-53 at IR-4 Control and Discussion, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

102. Through the “lessons learned process,” an organization should learn from past mistakes and prevent similar cyber threats moving forward. “The information accumulated from all lessons learned meetings [which an organization

should hold after major cybersecurity incidents] should be used to identify and correct systemic weaknesses and deficiencies in policies and procedures.” NIST-61 at p. 3, <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

103. The government has long recognized the importance of securing sensitive government data, and it requires contractors to take the appropriate steps to reasonably secure such information from malicious actors as required by the contracts and Government Cybersecurity Requirements. Indeed, the purpose of the Department of Justice False Claims Act initiative is to combat cyber fraud that could endanger sensitive government information and “combine the department’s expertise in civil fraud enforcement, government procurement and cybersecurity to promote the critical mission of combating new and emerging cyber-threats.” <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

B. Salesforce

104. Salesforce owns and operates cloud-based environments, products, platforms and software used by businesses and government agencies in their day-to-day operations ranging from small team operations to international operations. Salesforce is ranked 37 on Fortune’s 100 Fastest-Growing Companies list, and 137 on the Fortune 500 list. Its annual revenue for 2022 was \$26.492 billion, a nearly 25 percent increase from 2021 and a nearly 55 percent increase from 2020.

105. Technology has advanced to cloud computing. Salesforce represents that “[c]loud computing is a way to access information and applications online instead of having to build, manage, and maintain them on your own hard drive or servers. It’s fast, efficient, and [expected to be] secure.”

106. However, the General Services Administration (GSA) Cloud Information Center warns, “[w]hen it comes to cloud, security is always a concern.” Because of this, contractors offering cloud services to store government data are required to comply with Government Cybersecurity Requirements.

107. Salesforce represents “that the confidentiality, integrity, and availability of its customers’ information is vital to their business operations and success. Trust underpins our relationships with all our customers.” Its customers include thousands of government agencies, and hundreds of thousands of government employees who use Salesforce products.

1. GovCloud: Zero Trust Environment

108. Salesforce offers a cloud service known as “Salesforce Government Cloud” or “GovCloud,” specifically for use by government agencies and government contractors. Internally, Salesforce calls GovCloud “GIA,” “GIA1,” or “GIA2”.

109. Salesforce represents that GovCloud or GIA is “a unique, limited access Salesforce environment that is configured differently than other production

environments to meet stricter security requirements.” This environment consists of various GovCloud data centers or “pods” that store sensitive government data on GovCloud. These data centers have names such as “NA21,” “NA107,” and other similarly named data centers, starting with a prefix such as “NA” (i.e., North America).

110. Salesforce uses GovCloud to store and process data and electronic information generated under government contracts. GovCloud also stores sensitive information, including credentials (usernames, passwords, tokens and keys) known as “GovCloud secrets” used by government users to access Salesforce products.

111. Salesforce also represents that GovCloud is a “Zero Trust Environment” meaning that anyone—including any of the over 73,000 Salesforce employees—is a possible malicious actor. **“Zero Trust assumes that there is no traditional network edge;** networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.” (original emphasis)

112. Salesforce also represents that GovCloud is its “dedicated infrastructure” for use only by the government and government contractors and is intended “[t]o help meet the compliance needs of public sector organizations in the United States,” and “[d]ata is processed and stored solely within the

continental U.S., operated and supported by screened U.S. citizens as applicable.”

113. Access to GovCloud is required to be limited to individuals who have undergone special security processes and background checks, so, it is a violation of Government Cybersecurity Requirements to allow or enable unauthorized individuals to access GovCloud. With that in mind, Salesforce represents that all GovCloud users are authenticated, validated and authorized before gaining access to any application or data in GovCloud. Unauthorized access to sensitive government data jeopardizes national security, government programs and consumer protection, and the confidentiality of the sensitive data.

114. Salesforce further represents that “[c]ompliance and vulnerability reporting in GIA [or GovCloud] is far more robust and more scrutinized than any other environment; it is the most secure environment at Salesforce. Data in GIA is strictly kept in GIA, and many teams have no personnel with access to GIA.”

115. GovCloud is widely used by federal, state and local government account users and their contractors. For example, at least 68 federal government agencies use Salesforce GovCloud, including DOD, the State Department, DHS, DOJ, the VA, and other agencies with essential government functions.

116. Salesforce’s government contracts grew exponentially during the pandemic through GovCloud for COVID-19 tracing and vaccine management.

Only one year after the pandemic began, Salesforce had contracted with more than 150 organizations, which included government agencies as well as international organizations and healthcare organizations, to use Salesforce technology for COVID-19 tracking and vaccine management. To assist with these pandemic programs, Salesforce was responsible to securely acquire the sensitive medical information of individuals all over the world and securely transmit that information to government databases where the information was processed, transmitted or stored under government contracts.

2. Platforms/Products

117. Government agencies also contract with Salesforce for the use of Salesforce's own products such as Tableau, MuleSoft, Heroku and Slack, as well as third-party software and platforms such as Codecov, Zoom, HackerOne, and Splunk. Salesforce expanded its core cloud offerings by acquiring these other products, which are all available to government agencies that contract with Salesforce through GovCloud:

- Heroku in January 2011
- MuleSoft in May 2018
- Tableau in August 2019
- Slack in July 2021

118. According to Salesforce, these products “trusted by companies all over the world” have made Salesforce’s “ecosystem more attractive for developers to build on,” increasing the value of Salesforce’s cloud offerings.

119. Salesforce acquired Heroku in early 2011. Heroku is “a cloud platform that lets companies build, deliver, monitor and scale apps [applications].” Heroku allows customers to become “an apps company” through quickly getting the applications up and running on the internet, without the need for the customer to implement certain hardware or servers to launch the applications. Certain government agencies have relied upon Salesforce to implement COVID-19 vaccination applications in compliance with Government Cybersecurity Requirements.

120. Salesforce acquired MuleSoft in 2018. MuleSoft is an integration platform that allows customers to connect large swaths of data from any system and in any architecture or environment—including GovCloud. MuleSoft “enable[s] all enterprises to surface their data—regardless of where it resides—to deliver intelligent, connected customer experiences across all channels and touchpoints.”

121. Essentially, MuleSoft offers organizations greater computing power to go about their business and to connect their information in an integrated manner. Certain government agencies like the VA have relied upon Salesforce to merge and integrate VA hospital systems’ vast scope of HIPAA-protected patient health care

information to streamline and improve patient clinical outcomes in compliance with Government Cybersecurity Requirements.

122. Salesforce acquired Tableau in 2019. Tableau is an analytics platform for organizations and government agencies to analyze, explore and manage data. For example, Tableau allows users to generate large spreadsheets with data and to understand patterns and insights from that data.

123. Salesforce offers a panoply of Tableau products to government users including the Tableau Server. On information and belief, the Tableau Server is a product used by a predominant number of government agencies because it functions as a central repository for data and visualizations, allowing customers to work collaboratively across their organization or government agency. As with other Salesforce products, government agencies can choose to use the Tableau Server on-premises or through GovCloud.

124. On information and belief, Tableau houses millions of gigabytes of sensitive government data that government agencies seek to capture, visualize, analyze and apply; and Salesforce is responsible for contracts related to HIPAA-protected data and other data related to VA health services and for services related to all DOD facilities and bases worldwide. Government agencies such as these have relied upon Salesforce to implement such programs in compliance with Government Cybersecurity Requirements.

3. Cyber Response

125. Government agencies rely upon Salesforce's representations that it will identify, protect against, detect, respond to and recover from cyber incidents involving sensitive government data. Salesforce has numerous written policies to implement Government Cybersecurity Requirements. However, while Salesforce compliance looks good "on paper," it routinely violates these requirements, including its own written policies.

126. Salesforce has designated departments to respond to cyber incidents: the Salesforce Security Response Center ("SSRC") and the Critical Incident Center ("CIC"). These departments take on different roles in the event of a maximum or high severity incident.

127. SSRC contains Salesforce's Computer Security Incident Response Team ("CSIRT"). "CSIRT is the lead for all cybersecurity incident response within Salesforce." Specifically, CSIRT is responsible for detecting, escalating, and responding to security incidents internal to Salesforce, as well as identifying corrective actions.

128. SSRC also contains the Product Security Incident Response Team ("PSIRT") that, on information and belief, responds to vulnerabilities related to Salesforce products, including external attacks jeopardizing the security of those products.

129. Meanwhile, the Critical Incident Center contains a team called Unified Command (“UC”). Unified Command provides an “an enhanced executive response” and “is the lead for all incident communications” for those deemed the “most impactful critical incidents.” Unified Command is “responsible for providing a corporate-wide framework for the execution of world-class incident communications for technology issues.”

130. Salesforce’s Standard Operating Procedure for incident response, drafted to comply with NIST-61, establishes the minimum baseline procedures for security, privacy, and data integrity incident management and aligns with Salesforce’s overall written incident management policies.

131. A security incident at Salesforce can involve account user data or personal data. Account user data includes “all data, including all text, sound, video, or image files, and software, that are provided to Salesforce by, or on behalf of, a customer through their use of services provided by Salesforce.” Personal data, on the other hand, is “any information relating to an identified or identifiable natural person,” such as a name, online identifier or other identifying information.

132. When a security incident occurs, Salesforce’s written cyber incident response plan requires notification to CSIRT. CSIRT receives notifications of cyber events from alerts, emails to the security team, phone

calls to the security hotline, account users, Salesforce IT staff, and third parties such as through HackerOne reports.

133. HackerOne describes itself as the “world’s top ethical hackers.” Through this platform, HackerOne generates reports for Salesforce after its friendly hackers try to gain unauthorized access to GovCloud to find cybersecurity vulnerabilities.

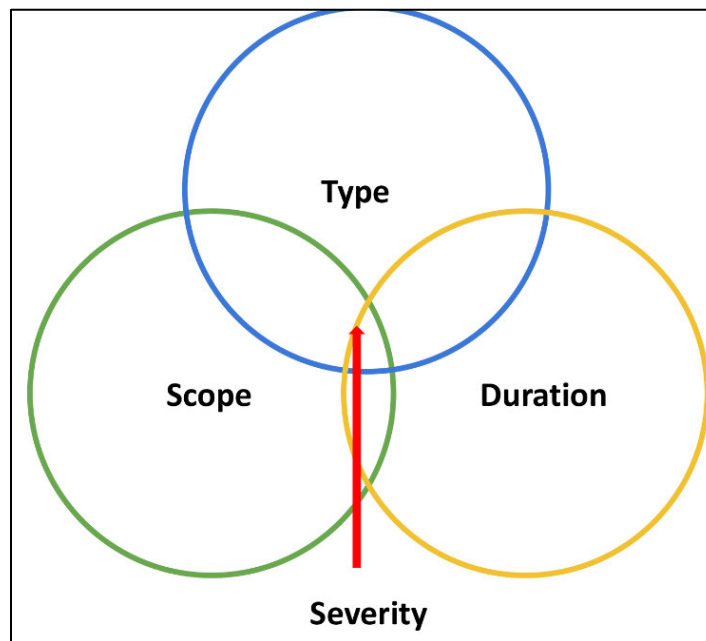
134. The security email account and hotline are run by Salesforce’s Information Security department, which sets internal security policies, fields complaints related to security issues, and addresses reported internal security violations. The Security Department, like CSIRT, is a part of the Salesforce Security Response Center (SSRC).

135. CSIRT sends incident notifications and subsequent updates to an internal Salesforce distribution list. These notifications and updates include the technical status update of the security response tasks but share information only on a need-to-know basis. These notifications and updates are referred to as “CSIRT critical vulnerability notifications.”

136. For communications to account users including government agencies, “[i]f there is impact to customers’ ability to access their org as a result of the security incident, . . . the messaging will remain very high level and not involve any details surrounding the cause of the ‘outage’. *[sic]*”

137. Certain categories of security incidents implicate additional response protocols. Security incidents that are labeled “Severity 0” or “Sev0” are deemed to be the most critical or maximum severity incidents. Incidents can also be labeled high severity, or “Severity 1” or “Sev1.” Salesforce also uses “P0” to identify cybersecurity vulnerabilities that should be handled as maximum priority. On information and belief, the labels Sev0 and P0 are synonymous and indicate a cyber incident that should be addressed as a critical and top priority.

138. The severity of an incident is determined at the cross-section of three critical inputs—scope, type, and duration of the incident:



139. Different products may have different triggers escalating the incident to Sev0. Specifically, CSIRT uses the following criteria to escalate a security incident to Sev0 or maximum severity:

- “Confirmed loss of confidentiality for ~ >50% of customer base for a service(s) or product(s); and exposure is external to Salesforce
- Confirmed loss of Integrity for ~ >50% of customer base for a service(s) or product(s)
- Business stopping and no acceptable workaround for >10 customers. Imminent threat to the business or near-term business milestone posing a financial risk
- Regulatory sanctions (e.g., debarment); or criminal charges; or financial restatement
- Severe damage to the Salesforce and/or a customer’s brand; or negative global attention; or substantial negative attention in key critical market space related to the public sector
- Customer(s) Impacted, likely to result in financial loss potentially impacting quarterly statements, severe regulatory sanctions; or global level reputational Impact.”

140. If CSIRT determines that the security incident is Sev0 or maximum severity, it should trigger collaboration with the Unified Command, which is slated to lead internal and external communications for Sev0 incidents. CSIRT are expected to remain involved in these communications as the subject matter expert.

141. A critical part of an effective cybersecurity program is the monitoring of logs. Logs are generated to record cyber activity or cyber events occurring within an organization's systems and networks. As described by NIST-92, "[m]any logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications. . . . Log management is essential to ensuring computer security records are stored in sufficient detail for an appropriate period of time." NIST-92 at ES-1, <https://csrc.nist.gov/publications/detail/sp/800-92/final>

142. Given the importance of logs in the oversight and management of an organization's system and network security, government contractors are required to ensure log "protect[ion] from breaches of their confidentiality and integrity." For example:

logs might intentionally or inadvertently capture sensitive information such as users' passwords and the content of e-mails. This raises security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through authorized or unauthorized means. Logs that are secured improperly in

storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party.

NIST-92 at 2-9 (Log Protection), <https://csrc.nist.gov/publications/detail/sp/800-92/final>

143. Salesforce leases a third-party software called “Splunk” to collect, store, monitor and analyze cyber activity logs for GovCloud, as well as its other cloud environments. Splunk store billions (and maybe trillions) of logs containing sensitive government data on GovCloud, including details related to access to sensitive government data, such as account users’ credentials (usernames, passwords, tokens and keys). For this reason, the importance of protecting the information in Splunk is as high as the protections needed for the same information stored in GovCloud. The usefulness of these logs to prevent cyberattacks and breaches or to mitigate harm to government agencies is dependent upon Salesforce’ vigilant analysis of accompanying logs.

144. Salesforce recognizes that serious incidents on GovCloud can have catastrophic consequences for government agencies:

- “[a]ny Government Cloud data that is outside of Government Cloud constitutes a security incident and **must be reported [to Salesforce Information Security] immediately.**”
- “the longer an attacker is on our network, the deeper they can go, the more backdoors they can deploy, and the more data they can exfiltrate.” (original emphasis)

145. Yet, as alleged in this Complaint, Salesforce routinely gave short shrift to its own written policies and violated Government Cybersecurity Requirements.

C. The Government Contracts

146. Salesforce contracts with federal, state and local government agencies, including agencies such as the U.S. Department of Defense, U.S. Department of State, U.S. Department of Veterans Affairs, and the U.S. Postal Service, for Salesforce cloud services and products such as GovCloud, Tableau, MuleSoft, and Heroku.

147. Salesforce contracts globally with over 250,000 customers and focuses its marketing efforts on larger enterprise customers like government agencies.

148. In fact, Salesforce now receives one billion dollars in annual revenue from thousands of accounts with government agencies.

149. Salesforce maintains over 10,000 “accounts” (defined as an organization or consumer for which Salesforce tracks activity and payments) with government agencies. Certain agencies have numerous accounts with Salesforce under more than one government contract. “Government users” or individual government employees access Salesforce products and services through these contracts under these “accounts.”

150. Salesforce contracted with government agencies for use of certain products, among them Tableau, MuleSoft, and Heroku, through numerous government accounts:

<u>Product</u>	<u>Number of Government Accounts</u>
Tableau	At least 1,185
MuleSoft	At least 75
Heroku	At least 115

151. Salesforce has also expanded its offerings to include storing and processing **classified** government information. In 2021, Salesforce contracted with the State Department to provide cloud services for “secret” government

information, including contact information, historical data, and other contextual information for more than 270 diplomatic posts globally. This State Department contract alone is worth at least tens of millions of dollars already and is projected to value several hundred million dollars. Salesforce is even exploring opportunities to house “top secret” government information that would require a SCIF (sensitive compartmented information facility) to access.

152. Federal, state and local government agencies have paid Salesforce billions of dollars to help manage, process, and confidentially store large volumes of sensitive government data with varying levels of classification.

153. Government account users rely on Salesforce to protect their sensitive data including the sensitive data of the beneficiaries of many government contracts.

1. Federal Contracts

154. The federal government has spent billions of dollars on Salesforce’s cloud services and other software products. The agencies rely on Salesforce to protect their sensitive government data in GovCloud and through their numerous platforms.

155. Salesforce has contracts with at least these federal agencies:

- U.S. Department of Agriculture (USDA)
- U.S. Department of Justice (DOJ)

- U.S. Department of Defense (DOD)
- National Aeronautics and Space Administration (NASA)
- U.S. Department of Veterans Affairs (VA)
- Federal Aviation Administration (FAA)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Labor (DOL)
- U.S. Department of Energy (DOE)
- U.S. Department of the Interior (DOI)
- U.S. Department of Housing and Urban Development (HUD)
- U.S. Department of the Treasury (DT)
- U.S. Department of Health and Human Services (DHHS)
- U.S. Department of Education (ED)
- U.S. Department of State (State Department)
- U.S. Department of Commerce (DOC)
- U.S. Department of Transportation (DOT)
- U.S. Environmental Protection Agency (EPA)
- U.S. Postal Service (USPS)
- U.S. Congress
- U.S. Peace Corps
- Corporation for National & Community Service (CNCS)

- U.S. Securities and Exchange Commission (SEC)
- Small Business Administration (SBA)
- Federal Communications Commission (FCC)
- Consumer Financial Protection Bureau (CFPB)
- Nuclear Regulatory Commission (NRC)
- Executive Office of the President (EOP)
- Commodity Futures Trading Commission (CFTC)
- Federal Deposit Insurance Corporation (FDIC)
- U.S. Agency for International Development (USAID)
- Centers for Medicare and Medicaid Services (CMS)
- National Archives and Record Administration (NARA)
- National Science Foundation (NSF)
- General Services Administration (GSA)
- U.S. International Trade Commission (ITC)
- Social Security Administration (SSA)

156. Many of these federal agencies maintain numerous accounts with Salesforce under multiple government contracts over multiple years, including these:

- 349 DOD accounts in the amount of at least \$40 million each year

- 56 State Department accounts in the amount of at least at \$11.25 million each year.
- 118 DHS accounts in the amount of at least \$23 million each year.
- 42 DOJ accounts in the amount of at least \$1 million each year.
- VA accounts in the amount of at least \$6.1 million each year.
- USPS accounts valued at least at \$17.8 million each year.

2. State/Local Contracts

157. Numerous states, the District of Columbia and New York City have also contracted with Salesforce for cloud services and products such as GovCloud, Tableau, MuleSoft, and Heroku.

158. Collectively, these states and localities spend at least \$56 million each year on Salesforce's cloud services and other software products, relying upon Salesforce to protect the sensitive data it is entrusted with under these government contracts.

159. The State of California has numerous government contracts with Salesforce with at least 230 accounts valued at over \$13.5 million each year, including for Salesforce products such as Tableau, MuleSoft, and Heroku.

160. The State of Delaware has contracted with Salesforce through at least 50 accounts worth at least \$2.3 million each year, including for Salesforce products such as Tableau and MuleSoft.

161. The District of Columbia has contracted with Salesforce through at least 100 accounts worth at least \$4.2 million each year, including for Salesforce products such as Tableau, MuleSoft, and Heroku.

162. The State of Florida has contracted with Salesforce through at least 120 accounts worth at least \$6 million each year, including for Salesforce products such as Tableau and MuleSoft.

163. The State of Hawaii has contracted with Salesforce through at least 50 accounts worth at least \$770,000 each year, including for Salesforce products such as Tableau and Heroku.

164. The State of Illinois has contracted with Salesforce through at least 80 accounts worth at least \$1.2 million each year, including for Salesforce products such as Tableau.

165. The State of Indiana has contracted with Salesforce through at least 100 accounts worth at least \$2.5 million each year, including for Salesforce products such as Tableau and MuleSoft.

166. The State of Iowa has contracted with Salesforce through at least 60 accounts worth at least \$600,000 each year, including for Salesforce products such as Tableau.

167. The Commonwealth of Massachusetts has contracted with Salesforce through at least 130 accounts worth at least \$1.8 million each year, including for Salesforce products such as Tableau, MuleSoft, and Heroku.

168. The State of Minnesota has contracted with Salesforce through at least 60 accounts worth at least \$640,000 each year, including for Salesforce products such as Tableau and Heroku.

169. The State of Montana has contracted with Salesforce through at least 30 accounts worth at least \$280,000 each year, including for Salesforce products such as Tableau and Heroku.

170. The State of Nevada has contracted with Salesforce through at least 60 accounts worth at least \$1 million each year, including for Salesforce products such as Tableau.

171. The State of New Jersey has contracted with Salesforce through at least 85 accounts worth at least \$3.1 million each year, including for Salesforce products such as Tableau and MuleSoft.

172. The State of New Mexico has contracted with Salesforce through at least 50 accounts worth at least \$1.5 million each year, including for Salesforce products such as Tableau and Heroku.

173. The State of New York has contracted with Salesforce through at least 140 accounts worth at least \$3.8 million each year, including for Salesforce products such as Tableau, MuleSoft, and Heroku.

174. New York City has contracted with Salesforce through at least 125 accounts worth at least \$6.4 million each year, including for Salesforce products such as Tableau, MuleSoft, and Heroku.

175. The State of North Carolina has contracted with Salesforce through at least 80 accounts worth at least \$2.9 million each year, including for Salesforce products such as Tableau.

176. The State of Rhode Island has contracted with Salesforce through at least 40 accounts worth at least \$400,000 each year, including for Salesforce products such as Tableau.

177. The State of Tennessee has contracted with Salesforce through at least 70 accounts worth at least \$2 million each year, including for Salesforce products such as Tableau.

178. The State of Vermont has contracted with Salesforce through at least 15 accounts worth at least \$400,000 each year, including for Salesforce products such as MuleSoft.

179. The State of Virginia has contracted with Salesforce through at least 70 accounts worth at least \$780,000 each year, including for Salesforce products such as Tableau.

180. To summarize, numerous States, the District of Columbia and New York City contract with Salesforce for its cloud services and products such as Tableau, MuleSoft, and Heroku as follows:

Product	State and Local Entities
Tableau	District of Columbia, New York City, and States of California, Delaware, Florida, Hawaii, Illinois, Indiana, Iowa, Massachusetts, Minnesota, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, Rhode Island, Tennessee, and Virginia
MuleSoft	District of Columbia, New York City, and States of California, Delaware, Florida, Indiana, Massachusetts, New Jersey, New York, and Vermont
Heroku	District of Columbia, New York City, and States of California, Hawaii, Massachusetts, Minnesota, Montana, New Mexico, and New York

IV. THE FRAUD SCHEME

181. Government agencies recognize the sensitive nature of certain government data and the potential consequences from unauthorized disclosures of sensitive data. It is for precisely this reason that Government Cybersecurity Requirements mandate that government contractors safeguard electronic systems that store such data, and adopt cybersecurity protections to identify, protect against, detect, respond to, and recover from cyber threats, cybersecurity events, cyber attacks and cyber incidents. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012); 81 Fed. Reg. 30439, at 30439

182. NIST defines cyber threats, events, attacks and incidents:

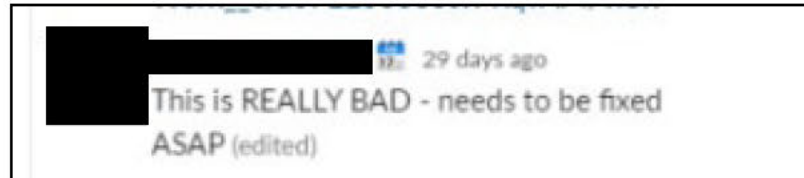
- A “cyber threat” is “[a]ny circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation” because of unauthorized access or disclosure, among others.
- A “cybersecurity event” is any “cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).”

- A “cyber attack” is an “attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.”
- A “cyber incident” involves “[a]ctions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.”

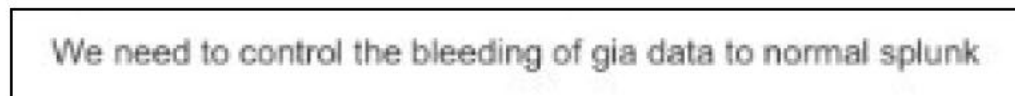
183. Salesforce knowingly failed to comply with Government Cybersecurity Requirements, triggering persistent and unabated cyber threats, cybersecurity events, cyber attacks, and cyber incidents that jeopardized massive amounts of sensitive government data. It was wholly unprepared to meet the five critical functions (identify, protect, detect, respond, recover), leaving it often ill-equipped to determine whether and what sensitive data was getting into the hands of malicious actors. It is not the existence of malicious or possible malicious actors but the consistent failure to properly act and the failure to make proper disclosures to the government agencies that gives rise to Salesforce’s False Claims Act liability.

184. Salesforce's violations ran the gamut from unaddressed software engineering failures that knowingly put government data at risk (e.g., Cyber Incident #6) to intentional whitewashing of known vulnerabilities (e.g., the Zoom cyber threat). It encompassed all its products, among them GovCloud, Tableau, MuleSoft, Heroku.

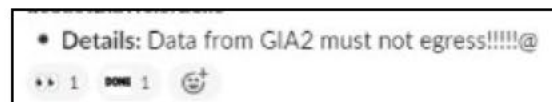
185. Salesforce knew its violations of Government Cybersecurity Requirements put government data at risk. For example:



186. And Salesforce knew its violations had a significant impact on government agencies:



187. Salesforce also knew the importance of Government Cybersecurity Requirements:



188. And Salesforce knew that its violations of Government Cybersecurity Requirements caused a “real problem” for government agencies:

update the topic information. Only a few topics are required, so our information must be specific and restrict access to only those topics.

- There is no room for mistakes in GIA as we don't have Topic Deployer config as a second layer of defense against mistakes. And accidentally sending data across the boundary is a real problem.

189. In some instances, Salesforce's knowing violations led to the **breach** of sensitive government data, defined by NIST as:

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: **a person other than an authorized user** accesses or potentially accesses personally identifiable information; or **an authorized user** accesses personally identifiable information for another than authorized purpose.

(emphasis added)

190. Sensitive government data with varying degrees of sensitivity were breached or made vulnerable to breach on Salesforce's watch:

- data about government agencies, operations, logistics
- internal government agency communications
- government employees' PII and login credentials (usernames, passwords, tokens and keys)
- the data of non-governmental businesses and private consumers such as patients, U.S. military members and veterans who are

the beneficiaries of certain government contracts with Salesforce

- detailed histories showing the activities of government employees on GovCloud, such as data accessed, reviewed, revised, shared (when and with whom)
- the names (or titles) and locations of government data, including documents, spreadsheets, presentations, memos, and other information stored on GovCloud
- details of government agency cyber vulnerabilities

191. Despite its knowing violations, Salesforce continued to solicit government contracts with false representations that its cybersecurity program was reliable and trustworthy:

Our comprehensive approach to data security is anchored by our core value, trust. We embed **robust security practices** across all of our technology, processes, and programs so that **public sector organizations can rely on us** to deliver high levels of confidentiality, integrity, and data availability.

(emphasis added)

192. On information and belief, Salesforce routinely made false or misleading statements to mollify government agencies:

- “not aware of any data loss at this time”
- “not aware of any malicious activity related to this issue at this time”
- “NEVER ALLUDE TO OR SUGGEST DATA LOSS DURING AN INCIDENT UNLESS TIC [Technical Incident Communications] HAS APPROVED RELEVANT LANGUAGE.” (original emphasis)

193. Because of its violations of Government Cybersecurity Requirements, Salesforce:

- knowingly exposed government data which included consumer data to possible malicious actors by enabling cloaked attacks through its platforms such as Tableau (e.g., Cyber Incident #1, Cyber Incident #2, Cyber Incident #3) and MuleSoft (e.g., Cyber Incident #4, Cyber Incident #5), and enabling conspicuous attacks (e.g., Cyber Incident #6, Cyber Incident #7, Cyber Incident #8)
- knowingly exposed government (and consumer) data to actual breaches, including breaches such as Cyber

Incident #9 that caused other serious cyber incidents (e.g., Cyber Incident #10, Cyber Incident #11, Cyber Incident #12, POLARIS), creating a disastrous domino effect like an unabated oil spill; and through platforms such as Heroku (Cyber Incident #13); and through third party software such as Codecov

- knowingly perpetuated imminent threats to the release of government (and consumer) data to unauthorized users through third party platforms such as Zoom.

194. Government agencies that contract with Salesforce are sitting ducks left vulnerable to malicious actors.

195. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims, and the government agencies paid those claims.

A. Knowingly Exposing Government and Consumer Data to Possible Malicious Actors

196. Salesforce's failure to comply with Government Cybersecurity Requirements enabled possible malicious actors to gain access to sensitive government data through various means. In some instances, Salesforce

enabled possible malicious actors to login to Salesforce products by using government employee credentials (usernames, passwords, tokens and keys), which allowed them to launch an attack under the cloak of an authorized government employee, i.e., a cloaked attack. At other times, possible malicious actors were not cloaked as authorized users, i.e., a conspicuous attack.

197. Cloaked attacks were made possible through Salesforce platforms such as Tableau, as shown by examples like Cyber Incident #1, Cyber Incident #2, and Cyber Incident #3. These examples demonstrate how sensitive government data was vulnerable to malicious actors unbeknown to the government agencies that contracted with Salesforce for use of Tableau.

198. Because of persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims, and the government agencies paid those claims.

1. Knowingly Enabling Cloaked Attacks

199. Salesforce knowingly enabled possible malicious actors to launch a cloaked attack on government agencies through Salesforce platforms such as Tableau and MuleSoft, i.e., possible malicious actors cloaked as authorized government users. It did so by allowing possible malicious actors to gain

access to government user credentials (usernames, passwords, tokens and keys) through improper and unsafe storage of user credentials. Armed with these credentials, malicious actors could have direct access to all data that was accessible to the government user. Through this vulnerability, the hacker would be cloaked as a government user, making it harder for the government to detect that an attack even occurred.

a. Tableau Platform

200. Salesforce acquired Tableau in August 2019, a platform to analyze, explore and manage data, allowing users to generate large spreadsheets to understand patterns and insights from the data. On information and belief, many government agencies also use the Tableau server as well as its data analytics tool. The server functions as a central repository for data and visualizations, allowing customers to work collaboratively across their organization either through the cloud or their own internal servers.

201. Numerous federal agencies contract each year with Salesforce for the use of Tableau through almost 2,000 government accounts, including at least 16 DHS contracts worth at least over \$17 million each year; at least 82 DOD contracts worth at least over \$27 million each year; and at least 10 DOJ accounts worth approximately one million dollars each year. And dozens of states and localities have government contracts for use of Tableau (e.g., California, Delaware, Florida,

Hawaii, Illinois, Indiana, Iowa, Massachusetts, Minnesota, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, Rhode Island, Tennessee, Virginia, the District of Columbia, and New York City).

202. As part of their usage, government agencies typically rely upon Tableau as a tool to analyze large quantities of their sensitive data uploaded to GovCloud or the Tableau server. In fact, on information and belief, Tableau houses millions of gigabytes of sensitive government data such as data related to DOD facilities and U.S. military bases worldwide and HIPAA-protected patient information related to the VA and DOD health care facilities, including the medical records of military members and their families, and veterans.

203. Yet despite this reliance by government agencies, on information and belief, Salesforce knowingly violated Government Cybersecurity Requirements involving Tableau, including failing to (a) investigate the full scope of such cyber incidents (e.g., failing to conduct a proper lookback), (b) notify customers about such incidents unless it was certain that the customer's data had been breached, and (c) review activity logs of GovCloud customers after cyber incidents, which means CIC was not in a position to know whether the cyber incident impacted government customers, which government customers were impacted, or what data was accessed. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

204. Government agency users of Tableau were impacted by Salesforce's violations of Government Cybersecurity Requirements, as shown by the below examples of cyber threats, events, attacks, or incidents codenamed Cyber Incident #1, Cyber Incident #2, and Cyber Incident #3.

(i) Cyber Incident #1

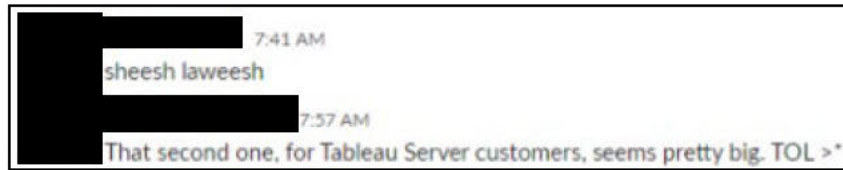
205. In June 2020, Salesforce discovered through a notification to CSIRT that a Tableau software "bug" caused by a Salesforce software coding error exposed government user credentials: "Keychain secrets including customer access tokens and username/passwords are exposed within the Tableau product." This incident exposed customer "data source credentials" to "an unintended audience", i.e., unauthorized users. This software bug caused Tableau to expose government user credentials to unauthorized data repositories where their credentials could be freely accessed by unauthorized users and possible malicious actors even after users changed their passwords as a security measure.

206. Salesforce gave this cyber incident the code name Cyber Incident #1 and rated it as the highest level of severity or Sev0.

207. Further, the impact to government agencies and consumers was readily apparent:



208. Salesforce employees immediately recognized the significant impact of this cyber incident:



209. Yet Salesforce was wholly unable to determine the timing or scope of the vulnerability and learned that it may have existed since as early as 2015:

- “[t]he current understanding [as of June 2020 was] that this impacts all Tableau customers.”
- “The bug appears to have been introduced in Tableau version 2018.1, which released in the first quarter of 2018.”
- “The current understanding is that this . . . appears to have been introduced in Tableau version 9.0 which was released in May 2015.”

210. Yet, despite not knowing whether a cloaked attack may have occurred as many as five years prior, Salesforce limited its lookback to 180 days.

211. Further, on July 7, 2020, Salesforce knowingly made misleading disclosures of information to affected government users (half-truths) when it notified only some affected customers and the information it did disclose was insufficient.

212. Even though months later (October 2020), Salesforce customers' login credentials continued to be vulnerable to possible malicious actors, Salesforce refused to give them the information they needed to safeguard their credentials ("with the [hyper password] issue, our Quip doc says not to give the location of the file out to the customer..."); and Salesforce was wholly unprepared to perform the work necessary to identify the customers impacted and the scope of the impact ("...so I'm looking for him. What am I looking for?"). Instead, Salesforce employees asked unauthorized users for guidance: "you are not really supposed to tell me if the customer's secrets were leaked, I think [...] but don't hesitate to ask for help."

213. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #1, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

214. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

(ii) Cyber Incident #2

215. On February 18, 2021, Salesforce again discovered another cyber incident involving the unauthorized disclosure of government user passwords involving Tableau, code named Cyber Incident #2. But it wasn't until March 9 that Salesforce made some disclosure of the incident to customers.

216. In response to one customer inquiry about this potential breach ("has this potential breach been logged officially with the ICO [the United Kingdom's Information Commissioner's Office]?"), Salesforce responded that:

We have no evidence of customer credentials having been shared outside of the Tableau environment or with any unauthorized third parties. [Salesforce] encourages customers to consult with their own legal counsel to determine whether they have any regulatory reporting obligations under applicable laws. . . .

217. On information and belief, Salesforce's representation was knowingly misleading because its only purpose was to mollify the customer with no basis for the factual information provided to the customer.

218. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #2, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible

malicious actors. 48 C.F.R. § 52.204-21 (FAR Safeguarding Requirements); 48 C.F.R. § 252.204-7012 (DFARS 7012)

219. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

(iii) Cyber Incident #3

220. On December 5, 2021, a customer reported to Salesforce that GovCloud was vulnerable to attack through the Tableau platform, “but a root cause analysis was not performed” and Salesforce ignored this customer report.

221. Three months later, on March 12, 2022, a Salesforce contractor responsible to identify cybersecurity risks (i.e., a “friendly” hacker) also discovered a “broken access control vulnerability” when he gained unauthorized access to GovCloud through the Tableau platform. This vulnerability allowed possible malicious actors to grant access to certain users and change login credentials: “[i]f exploited, this issue could permit access to any data or information accessible by the targeted user.” Salesforce gave this incident the code name Cyber Incident #3.

222. Salesforce further learned that GovCloud had been vulnerable to attack through the Tableau platform as early as December 7, 2015, but it failed to

determine the nature or scope of the risk. “Due to the nature of this vulnerability, it is not possible to easily differentiate between authorized and malicious activity, making it difficult to identify evidence of exploitation.”

223. Further, on March 24, 2022, Salesforce shared only limited information with certain government agencies, thereby making a knowingly misleading disclosure to the government. Salesforce notified only those customers who “may need to update” Tableau and waited two months to post a brief advisory about the cybersecurity vulnerability online on May 23, 2022: “The vulnerability allows a malicious site administrator to change passwords for users in different sites hosted on the same Tableau Server, resulting in the potential for unauthorized access to data.”

224. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #3, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

225. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

b. MuleSoft Platform

226. Salesforce acquired MuleSoft in 2018, an integration platform that allows customers to connect large swaths of data from any system and in any architecture or environment—including GovCloud, “enable[ing] all enterprises to surface their data—regardless of where it resides—to deliver intelligent, connected customer experiences across all channels and touchpoints.”

227. Government agencies have relied upon the MuleSoft platform to process and store their data efficiently and securely. For example, the VA has relied upon MuleSoft to merge and integrate HIPAA-protected medical records of patients under the care of the VA hospital system to streamline and improve patient clinical outcomes.

228. Numerous federal agencies contract each year with Salesforce for the use of MuleSoft products through at least 75 government accounts, including at least 3 DHS accounts worth at least \$7 million each year; at least 5 DOD accounts worth at least over \$12 million each year; and at least 2 State Department accounts worth over one million dollars each year. And nearly a dozen states and localities have government contracts for use of MuleSoft (e.g., the District of Columbia, New York City, California, Delaware, Florida, Indiana, Massachusetts, New Jersey, New York, and Vermont).

229. Yet despite this reliance by government agencies, on information and belief, Salesforce knowingly failed to comply with Government Cybersecurity Requirements involving MuleSoft, including failing to (a) prevent cyber incidents in the first place, (b) investigate the full scope of the impact once the incident occurred, (c) identify all customers and their data affected, and (d) properly inform the affected government agencies. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

230. Government agency users of MuleSoft were impacted by Salesforce’s violations of Government Cybersecurity Requirements, as shown by the below examples of cyber threats, events, attacks, and incidents code named Cyber Incident #4 and Cyber Incident #5.

231. More specifically, on April 9, 2020, Salesforce was notified of two GovCloud vulnerabilities through the MuleSoft platform by HackerOne—a “friendly” third party hacker.

(i) Cyber Incident #4

232. In the first incident on April 9, 2020, a MuleSoft vulnerability allowed unauthorized users to “buy . . . ip [internet protocol] addresses and takeover full control of the domain,” enabling possible malicious actors to spoof the website domain demo.mulesoft.com—a website that demonstrates the uses of MuleSoft and hosts its own content—and redirect control of the site to the actor without user

knowledge; install a virus on GovCloud for any government agency user who accessed the site; or track the GovCloud activity of the government users.

Troublingly, “[t]he victim has no way of telling, whether the content is served by the domain or the cyber attacker.”

233. Salesforce gave this cyber incident the code name Cyber Incident #4 and rated it the highest priority level or P0.

234. Yet in response to this incident, Salesforce knowingly violated Government Cybersecurity Requirements because despite the discovery of the spoofed domain, it failed to investigate the incident, identify the data at risk, and notify government users whose accounts may have been accessed by unauthorized users. “CSIRT determined that log review for previous exploitation is not possible for commercial and GIA [GovCloud] environments.”

235. Further, in violation of Government Cybersecurity Requirements, Salesforce knowingly failed to (a) investigate the full scope of the impact once the incident occurred, i.e., perform an historical lookback (b) identify all customers and their data affected, or (c) properly inform the affected government agencies.

236. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #4, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible

malicious actors. 48 C.F.R. § 52.204-21 (FAR Safeguarding Requirements); 48 C.F.R. § 252.204-7012 (DFARS 7012)

237. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

(ii) Cyber Incident #5

238. The second cyber incident on April 9, 2020, involved MuleSoft's Connected App feature, which connects external applications to those within a user's network. Salesforce represented that this feature had a restricted access function that prevented applications from collecting external information or acting outside of allowable parameters.

239. However, restricted applications were granted privileges (i.e., special authorization granted to certain users to perform security relevant operations), allowing hackers to gain access to user information, including credentials (usernames, passwords, tokens and keys) that were viewable in logs that should have themselves been inaccessible, extract private data, and even write new content to change how the software operates. A malicious actor could misappropriate and use government employee credentials "to perform privileged stateful actions [i.e., actions dependent on external rather than self-contained data

stores] within MuleSoft, which would allow the Connected App to escalate privileges from hereon indefinitely,” jeopardizing the security of sensitive government data.

240. Salesforce gave this cyber incident the code name Cyber Incident #5 and rated it the highest priority level or P0.

241. Yet in response to this information, Salesforce did nothing: “The [cyber incident] detection was not possible due to lack of logs, this would also make it impossible to detect this issue during a historical search.”

242. Further, in violation of Government Cybersecurity Requirements, Salesforce knowingly failed to (a) investigate the full scope of the impact once the incident occurred, i.e., perform an historical lookback (b) identify all customers and their data affected, and (c) properly inform the affected government agencies.

243. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #5, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

244. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or

fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

2. Knowingly Enabling Conspicuous Attacks

245. Salesforce's failure to comply with Government Cybersecurity Requirements also enabled possible malicious actors to gain access to sensitive government data through means other than cloaked attacks. Some attacks on GovCloud were conspicuous, meaning the actors were not hiding behind authorized user credentials.

246. Conspicuous attacks were shown by examples such as Cyber Incident #6, Cyber Incident #7, and Cyber Incident #8. These examples demonstrate how government agencies that contracted with Salesforce unwittingly left their sensitive government data at risk to possible malicious actors.

247. And government agencies that contracted for the use of GovCloud (a/k/a GIA) relied upon Salesforce's written policies to provide heightened protections for sensitive government data stored in GovCloud such as segregating the data from more widely accessible environments outside of GovCloud:

- “[a]ny Government Cloud data that is outside of Government Cloud constitutes a security incident and **must**

be reported [to Salesforce Information Security] immediately.”

- “if you see any Government Cloud data displayed outside of Government Cloud, this constitutes a security incident and it’s critical that you report it immediately . . .”
- “the longer an attacker is on our [GovCloud] network, the deeper they can go, the more backdoors they can deploy, and the more data they can exfiltrate.” (original emphasis)

248. Because of persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims, and the government agencies paid those claims.

a. Cyber Incident #6

249. In March 2022, Salesforce discovered a “data leak incident” or spillage of Splunk logs— records of cyber activity or cyber events —that “were inadvertently ingested into a location outside of the GovCloud boundary,” in violation of the Government Cybersecurity Requirements. Salesforce rated this cyber incident as the highest level of severity or Sev0.

250. Salesforce wasn’t aware of this cyber incident when it was occurring, but merely stumbled across the spilled data during a separate investigation of

another cyber incident: “CCE team discovered that NA107 [GovCloud] data is accessible during one investigation related to MQ/ASync [separate, unrelated investigation].”

251. However, government contractors like Salesforce are required to ensure log “protect[ion] from [such] breaches of their confidentiality and integrity”:

logs might intentionally or inadvertently capture sensitive information such as users’ passwords and the content of e-mails. This raises security and privacy concerns involving both the individuals that review the logs and others that might be able to access the logs through authorized or unauthorized means. Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction. This could cause a variety of impacts, including allowing malicious activities to go unnoticed and manipulating evidence to conceal the identity of a malicious party.


NIST SP 800-92 at 2-9 (Guide to Computer Security Log Management),

<https://csrc.nist.gov/publications/detail/sp/800-92/final>

252. Yet over an approximate 9-day span, GovCloud Splunk logs were spilled into unsecure cloud environments over 32 million times, making an enormous amount of sensitive government data accessible to unauthorized individuals and possible malicious actors; directly impacting the sensitive data of at least 100 government agencies: “*any customer who sent an email in last nine days would be impacted so it should be most of the customers*” (original emphasis).

253. And Salesforce knew that because “this incident involves GovCloud data,” it was a significant incident that required it to “discuss[] engaging additional GovCloud resources and how to ensure non-GovCloud engineers [i.e. unauthorized individuals] don’t access the GovCloud data.”

254. It also knew that storage of GovCloud data in non-GovCloud environments was a security breach:

 10 months ago

That would be almost certainly, a security breach. In fact, if GIA2 secrets have been pushed to global vault I suggest you engage CSIRT and notify as the secrets may have to be rotate asap

255. Yet Salesforce did nothing. As shown by this one example, Salesforce routinely failed to identify even widescale cyber incidents that affected all GovCloud customers.

256. On information and belief, in violation of Government Cybersecurity Requirements, Salesforce knowingly failed to (a) prevent the incident in the first

place, (b) investigate the full scope of the impact once the incident occurred, (c) identify all customers and their data affected, and (d) properly inform the affected government agencies.

257. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #6, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

258. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

b. Cyber Incident #7

259. During the first quarter of the 2022 fiscal year, Salesforce discovered at least 40 cyber incidents that exposed sensitive government data on GovCloud, with at least 8 GovCloud cyber incidents left unresolved by the end of the quarter.

260. In one example, in March 2020, Salesforce violations of Government Cybersecurity Requirements led to the exposure of the names (or titles) of all Google Doc(s) in GovCloud to unauthorized users, while acknowledging that “[t]his could result in unauthorized external access and exfiltration of customer

data.” Salesforce gave this cyber incident the code name Cyber Incident #7 and rated it the highest priority level or P0.

261. Yet in response to this incident, Salesforce did nothing: “[h]istorical review for exploitation of this vulnerability is not possible,” leaving a troubling question mark on which “unauthorized external access and exfiltration” of data could have occurred.

262. Further, on information and belief, in violation of Government Cybersecurity Requirements, Salesforce knowingly failed to (a) prevent the incident in the first place, (b) investigate the full scope of the impact once the incident occurred, (c) identify all customers and their data affected, and (d) properly inform the affected government agencies.

263. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #7, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors. 48 C.F.R. § 52.204-21 (FAR Safeguarding Requirements); 48 C.F.R. § 252.204-7012 (DFARS 7012)

264. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

c. Cyber Incident #8

265. In yet another incident this same month (March 2020), Salesforce knowingly provided possible malicious actors a roadmap to accessing sensitive government data to anyone on the internet through its own software engineering failure. Salesforce made “listviews” visible to “all external users” outside GovCloud by setting it “by default to be public.” Listviews expose the nesting hierarchy or mapping of the locations where sensitive government data reside. And, by exposing this information to “all external users,” possibly any user of the internet could access this roadmap and government data.

266. Salesforce gave this cyber incident the code name Cyber Incident #8 and rated it the highest priority level or P0.

267. And, on information and belief, Salesforce failed to notify customers about the cyber incident and intentionally avoided such obligations by downplaying the severity of the incident.

268. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #8, in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors. 48 C.F.R. § 52.204-21 (FAR Safeguarding Requirements); 48 C.F.R. § 252.204-7012 (DFARS 7012)

269. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

B. Knowingly Exposing Government and Consumer Data to Actual Breaches

270. Salesforce's violations of Government Cybersecurity Requirements exposed sensitive government data to actual breaches.

271. An actual breach is the compromise, unauthorized disclosure, or similar occurrence whereby any person other than the authorized user accesses (or potentially accesses) personally identifiable information (PII), defined as any information that can be used to distinguish or trace an individual's identity. Basic identifying information like a name or birth date is considered PII, as well as other sensitive information like social security numbers.

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: **a person other than an authorized user** accesses or potentially accesses personally identifiable information; or **an authorized user**

accesses personally identifiable information for another
than authorized purpose.

(emphasis added)

272. For example, Salesforce failed to properly address a 2019 breach of sensitive government data codenamed Cyber Incident #9—one of the most serious cyber incidents in Salesforce history. As a result, Cyber Incident #9 continually reared its head in the form of lingering vulnerabilities and subsequent cyber breaches until at least early 2022. These further cyber incidents included Cyber Incident #10, Cyber Incident #11, Cyber Incident #12, and POLARIS.

273. The breaches stemming from Cyber Incident #9 connected to the way in which data was transferred between various sources—a critical function necessary to ensure sensitive data is transferred securely and not susceptible to malicious actors while in transit. For at least three years, from 2019 through 2022, Salesforce played a game of whack-a-mole by responding piecemeal to each cyber incident.

274. And because it knowingly failed to identify, protect against, detect, respond to, and recover from such cyber incidents, Salesforce exposed sensitive government data to possible malicious actors.

275. Salesforce's failure to take affirmative steps to address continual and persistent cyber incidents had the effect of a disastrous oil spill. Failure to clean up

the first oil spill created a bigger challenge to contain and control the later oil spills.

276. Government agencies that contract with Salesforce are sitting ducks left vulnerable to malicious actors.

277. Because of persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

1. Cyber Incident #9

278. On or around April 8, 2019, Salesforce discovered one of the most serious of all its cyber incidents. Salesforce gave this cyber incident the code name Cyber Incident #9 and rated it the highest priority level or P0.

279. A significant volume of sensitive government data on GovCloud such as login credentials and first and last names, email addresses, and other PII of government users was leaked outside of the secure GovCloud environment. External users—non-Salesforce staff and guests (i.e., temporary users such as individuals who were trying a Salesforce product or software demo) were able to (and did) access this leaked sensitive information through numerous access points.

280. Yet Salesforce was wholly unprepared to address this cyber incident in violation of Government Cybersecurity Requirements despite its attempt to have a team address it.

281. Further, because of Salesforce's knowing failure to respond properly to Cyber Incident #9 when first discovered, Cyber Incident #9 caused other cyber incidents through 2022, creating a disastrous domino effect. These included Cyber Incident #10, Cyber Incident #11, Cyber Incident #12, and POLARIS.

282. Salesforce's routine failure to take affirmative steps to remedy cyber incidents had the effect of a disastrous oil spill. Failure to clean up the first oil spill created a bigger challenge to contain and control the later oil spills.

283. As a result of these breaches, Salesforce knowingly submitted false or fraudulent claims to government agencies, submitted false records material to fraudulent claims, and the government agencies paid those claims.

a. Cyber Incident #10

284. Salesforce knowingly failed to properly address Cyber Incident #9, in violation of Government Cybersecurity Requirements. Because of this, Cyber Incident #9 caused a domino effect of further cyber incidents. For starters, throughout January 2020, Salesforce discovered at least 72 access points in which possible malicious actors could gain access to an undetermined amount of sensitive government data.

285. Salesforce gave this cyber incident the code name Cyber Incident #10 and rated it the highest priority level or P0.

286. On January 5, 2020, Salesforce documented (or logged) over 65 separate CSIRT critical vulnerability notifications, all assigned the highest priority level or P0. Upon investigation, Salesforce found that the “P0’s [vulnerability notifications] related to [Cyber Incident #9]” resulted in over 50 unsecure access points that “allow[ed] unauthorized access” to external users and “Guest[s]” anywhere in the world. As such, possible malicious actors could gain access cloaked as a “whitelisted” system component (i.e., authorized components that were “on the list” to deal with certain information) thereby “expos[ing] [government] customer data”—again, unbeknown to government agencies.

287. Again, on January 21, 2020, Salesforce found an additional 22 access points “currently exploitable by external users.”

288. On information and belief, this January 21 event led to a known government data breach. Salesforce improperly limited its lookback to only 30 days.

289. Further, on information and belief, Salesforce knowingly violated Government Cybersecurity Requirements, including failing to (a) investigate the full scope of such cyber incidents (e.g., failing to conduct a proper lookback), (b) notify customers about such incidents unless it was certain that the customer’s data

had been breached, and (c) review activity logs of GovCloud customers after cyber incidents, which means CIC was not in a position to know whether the cyber incident impacted government customers, which government customers were impacted, or what data was accessed.

290. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #9, in violation of Government Cybersecurity Requirements. These violations led to continual breaches of sensitive government data to possible malicious actors through further level P0 cyber incidents like Cyber Incident #10. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

291. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

b. Cyber Incident #11

292. Yet again, in February 2020, a third party (HackerOne) report alerted Salesforce that government user credentials and PII continued to be exposed to unauthorized individuals.

293. Salesforce gave this cyber incident the code name Cyber Incident #11 and rated it the highest priority level or P0.

294. Salesforce knew that its failure to properly remedy the 2019-2020 Cyber Incident #9 led to Cyber Incident #11—10 months later (Apr. 2019 to Feb. 2020): the critical update “pushed [as a “PII fix”] in the past [2019] is found to be ineffective here.” This 10-month delay in appreciating that its Cyber Incident #9 fix was a failure, which left a gaping cyber hole open, is itself evidence of serious violations of Government Cybersecurity Requirements.

295. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #9, in violation of Government Cybersecurity Requirements. These violations led to continual breaches of sensitive government data to possible malicious actors through further level P0 cyber incidents like Cyber Incident #11. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

296. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

c. Cyber Incident #12

297. Further still, in July 2020, Salesforce discovered that the gaping hole left by Cyber Incident #9 “potentially impacted” the GovCloud data of thousands

of government employees of at least 32 government agencies. But Salesforce confirmed that data for 13 of the 32 agencies were actually breached.

298. More particularly, Salesforce discovered that government “custom profiles” were leaked onto the internet. Custom profiles define how users access data on GovCloud and serve as a vehicle or pipeline to connect application and data sources, (normally) allowing sensitive information to securely transfer between various data sources. This serves a critical function to allow two products to communicate with user interface endpoints, or end locations, where data is securely transferred. Put simply, access to government custom profiles was just another way for possible malicious actors to access government data.

299. The open access to these pipelines (i.e., custom profiles)—just like an open bank vault—enabled unauthorized individuals to access government data.

300. Salesforce gave this cyber incident the code name Cyber Incident #12 and assigned it the highest priority level or P0.

301. Further, despite the significance of the known “potential impact” to all 32 government agencies, Salesforce provided “white glove” treatment to only 13 or so of the 32 agencies, i.e., notice to the agencies that their accounts were accessed by unauthorized and possible malicious actors.

302. In its review of Cyber Incident #12, Salesforce further uncovered that the scope of the exposure of government custom profiles on the internet was even more massive than it originally understood.

303. Years before Cyber Incident #12, customers had already reported that custom profiles were accessible on the internet. For example, in September 2019, a customer reported that standard and custom profiles names were being disclosed to unauthenticated users, and Salesforce determined at that time that the issue affected all customers with force.com pages publicly available. Yet it was not until July 2020 that Salesforce discovered the potential impact to all 32 GovCloud customers; or the actual data breach of 13 of those.

304. In fact, because of Salesforce violations of Government Cybersecurity Requirements, on information and belief, government custom profiles were accessible to malicious actors on the internet at least as far back as 2017.

305. Yet Salesforce knowing failed to even attempt to remedy the vulnerability until February 2021—7 months after the notification: “fix [was] scheduled to be released in February 2021”.

306. Further, on information and belief, while Salesforce performed a superficial review of logs, it violated Government Cybersecurity Requirements, including failing to (a) investigate the full scope of the impact to adequately determine whether data from all 32 agencies was breached (e.g., failed to conduct a

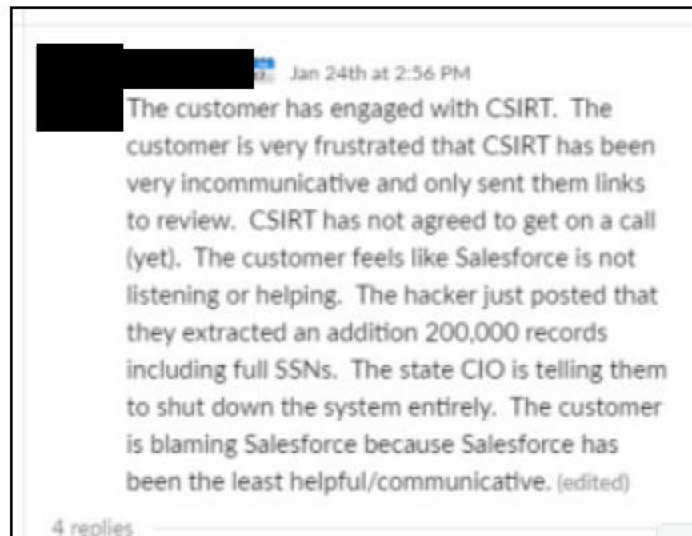
proper lookback), (b) notify customers about such incidents unless it was certain that the customer's data had been breached, and (c) review activity logs of GovCloud customers after cyber incidents, which means CIC was not in a position to know whether the cyber incident impacted government customers, which government customers were impacted, or what data was accessed.

307. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #9. These violations of Government Cybersecurity Requirements led to continual breaches of sensitive government data to possible malicious actors through further level P0 cyber incidents like Cyber Incident #12. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

308. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

d. POLARIS

309. Salesforce was routinely surprised by breaches reported by government customers rather than in control of its cybersecurity obligations to the government, and routinely failed to appreciate the magnitude and severity of such breaches:



On information and belief, this breach also traced back to Salesforce's original and continuing failure to take appropriate action in response to Cyber Incident #9.

310. Salesforce knowingly failed to identify, protect, detect, respond, and recover from Cyber Incident #9, in violation of Government Cybersecurity Requirements. This failure continued to expose sensitive government data to possible malicious actors through further serious cyber incidents like the POLARIS breach. 48 C.F.R. § 52.204-21 (FAR Safeguarding Requirements); 48 C.F.R. § 252.204-7012 (DFARS 7012)

311. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

2. Cyber Incident #13

312. Salesforce’s knowing violations of Government Cybersecurity Requirements also rendered GovCloud a sitting duck for a serious data breach in 2022 in which malicious actors stole—and used—government customer credentials from Salesforce’s Heroku platform. This gave possible malicious actors direct access to GovCloud through Heroku.

313. In addition to Tableau and MuleSoft, Heroku is a third cloud product that government agencies contract with Salesforce to use. Heroku “lets companies build, deliver, monitor and scale apps [applications].” Government agencies rely on Heroku to allow them to efficiently and securely get applications up and running on the internet, without the need for the agencies to implement their own hardware or servers to launch the applications.

314. On April 13, 2022, Salesforce discovered that a possible malicious actor had gained access to all or “a significant portion” of Heroku’s source code, which it stores on a proprietary development platform called GitHub, making it an easy target for possible malicious actors to infiltrate GitHub for future attacks.

315. Salesforce gave this cyber incident the code name Cyber Incident #13 and rated it the highest severity level or Sev0.

316. Through the stolen source code, the malicious actor was able to steal authentication information known as OAuth tokens, which then allowed it to hack into thousands of customer sites, including through GovCloud, and extract further government data.

317. Salesforce only discovered that source code had been stolen five days after an unauthorized individual logged into GitHub with a stolen OAuth token. The hacker had “obtained access to a Heroku database and downloaded stored customer GitHub integration OAuth tokens.”

318. Described another way, Salesforce discovered money missing from a bank vault; but only five days after the bank vault’s security system had failed. For this reason, the timing of the Salesforce discovery of the breach itself demonstrated a failure to comply with Government Cybersecurity Requirements.

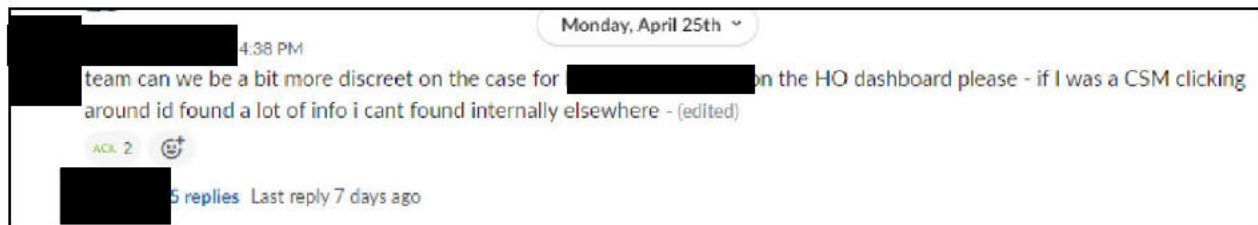
319. Only after having been under attack for as many as five days did Salesforce staff recognize the sheer magnitude of this breach:

- This is “[a] real [breach], probably the worst I’ve seen here . . . I never thought I’d face an incident like this in my career, but here we are.”
- “it’s looking like this [reaction to Cyber Incident #13] will be a long-running all-nighter for [Salesforce employee] and could

very well become our focus for several days, perhaps even the weekend.”

- We need to “call on more folks than usual to be ready to jump on the pager to provide coverage for your fatigued peers.”

320. Despite the significant potential impact to customers, Salesforce intentionally kept the news a close hold: “I can’t share many details about the incident right now except with folks who are/have responded to it – at least not in writing.” Senior Director of CIC implored members of his team to “be a bit more discreet”:



321. Yet there was impact felt by Heroku customers as shown by increasing complaints that were being made to Salesforce during this time:

Date	Number of Customer Cases
April 18, 2022	538
April 19, 2022	845
April 20, 2022	1,056
April 21, 2022	1,162

April 25, 2022	1,651
April 26, 2022	1,820
April 27, 2022	1,924

322. Notwithstanding clear evidence that government user credentials had been breached, Salesforce intentionally downplayed the cyber incident, notifying customers through a blog post on June 14, 2022, that (a) had “rotate[d]” their credentials only “out of an abundance of caution”, and (b) ha[d] no evidence of any unauthorized access to Heroku systems by this actor since April 14, 2022,” despite insufficient information to make that latter representation.

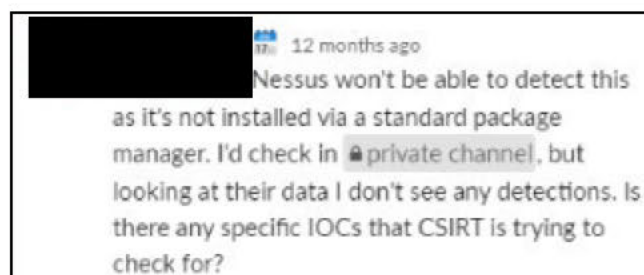
323. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from Cyber Incident #13, in violation of Government Cybersecurity Requirements. These violations led to continual breaches of sensitive government data to possible malicious actors. 48 C.F.R. § 52.204-21 (FAR Safeguarding Requirements); 48 C.F.R. § 252.204-7012 (DFARS 7012)

324. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

3. Codecov

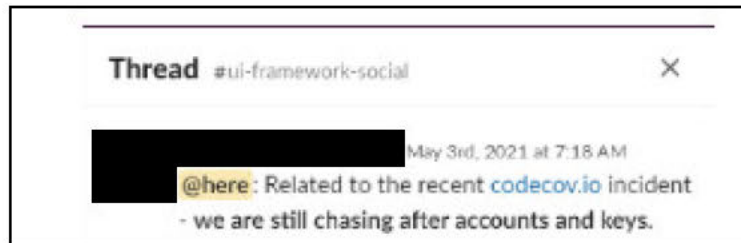
325. Even before the massive data breach known as Cyber Incident #13, Salesforce violations of Government Cybersecurity Requirements led to breach of government data on GovCloud at least one year earlier—in April 2021—through a leased third-party software program called Codecov. An unauthorized user gained access to Codecov, which is a code analytical tool that provides insight into the quality of a software program’s code, allowing the creation of “healthier code, faster, and with less risk”; and is proprietary software code for government agencies, government user credentials and government data.

326. Because of its violations of Government Cybersecurity Requirements, Salesforce could not “scan GovCloud environments for the recent security incident” and was thus unable to identify, investigate, or abate this continuing vulnerability in GovCloud:

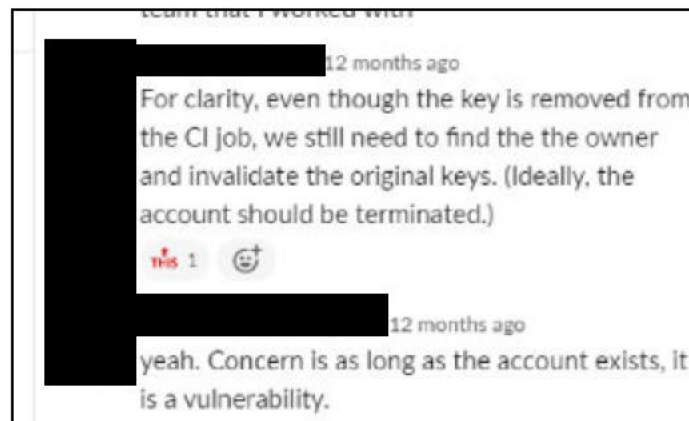


327. Because Salesforce also failed to identify the scope of Codecov’s use among its 73,000 employees, three weeks after its already-late discovery of the Codecov hack, Salesforce still had not appreciated that malicious actors had

breached government data (and may have continued to do so over the course of the previous three weeks). It also failed to identify the scope of the breach, including the government agencies that were affected:

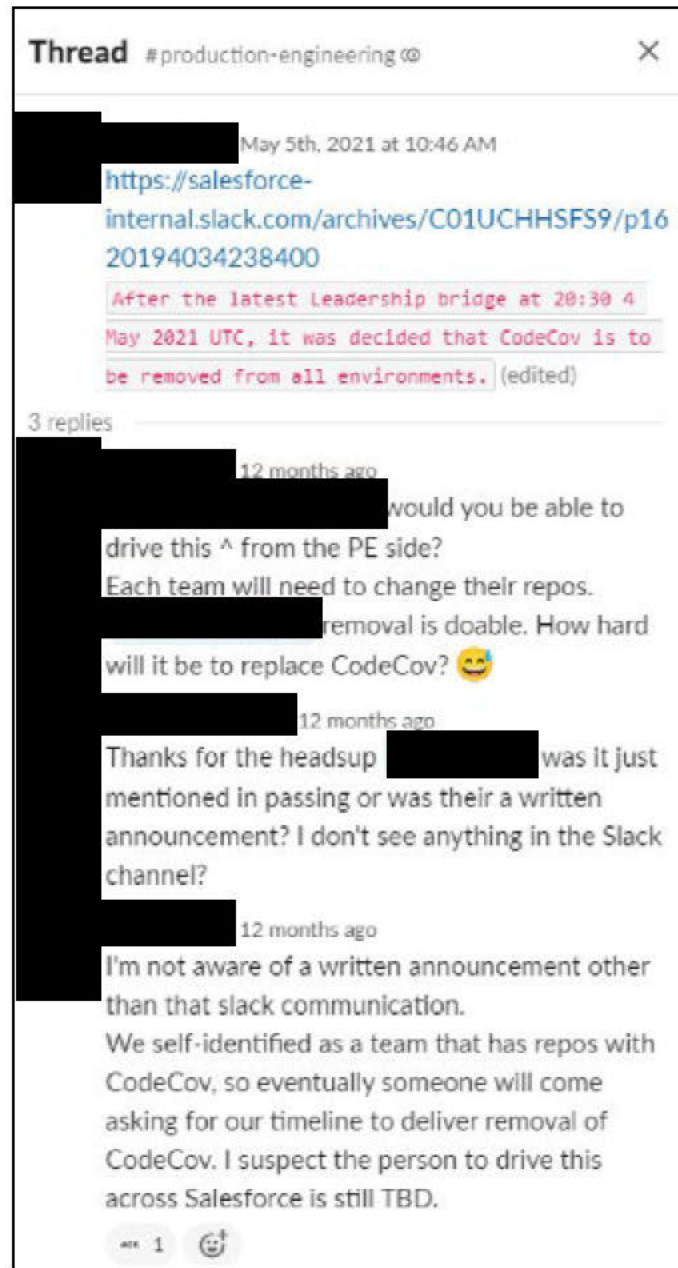


328. And Salesforce understood its actions in response were insufficient to avoid continual leaks of government data to the internet:

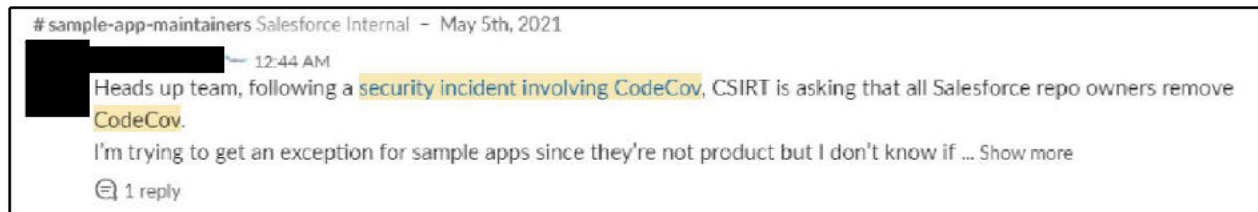


329. Thus, three weeks after discovery of the Codecov vulnerability, Salesforce knew that GovCloud data was still being breached.

330. Rather than implement cybersecurity measures, Salesforce failed to take steps to notify necessary team members of the continuing vulnerability from the Codecov software. Salesforce left communication about this serious vulnerability to travel word-of-mouth:



331. And rather than implement cybersecurity measures, Salesforce placed the onus on Salesforce employees to remove the Codecov software themselves at their discretion:



332. Salesforce failed to provide sufficient notice to the hundreds of customers whose data was at risk: “While we have no evidence at this time of unauthorized access to customer data, we continue to explore the full impact of the issue”

333. Salesforce also failed to address the system-wide vulnerability caused by the Codecov attack, instead choosing to “close” the CSIRT critical vulnerability on individual accounts on an ad hoc basis.

334. Seven months after the initial notification of a Codecov cyber incident in April 2021, Salesforce failed to inform its employees about the continuing vulnerability, so they continued to use the Codecov tool until at least as late as November 2021: “my codecov reports never get processed [] any ideas why? Further, Salesforce failed to properly remove, replace and repair (“patch”) the Codecov tool. Because of this, Salesforce has enabled another serious vulnerability to remain active in GovCloud, which continues to expose government data to possible malicious actors.

335. Salesforce knowingly failed to comply with Government Cybersecurity Requirements, including failing to (a) prevent the incident in the

first place, (b) investigate the full scope of the impact, (c) identify all customers and their data affected, or (d) properly inform the affected government agencies.

336. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from the cyber incident relating to the Codecov tool, in violation of Government Cybersecurity Requirements. These violations led to continual breaches of sensitive government data to possible malicious actors. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

337. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

C. Knowingly Perpetuating Imminent Threats to Government and Consumer Data

338. Salesforce's violations of Government Cybersecurity Requirements extended to its failures to perform the most basic and commonsense protections for the credentials and privileges of its own employees working on the government contracts. Salesforce's knowing failures to ensure the authenticity and authorization of its own employees opened the door for possible malicious actors to launch cloaked attacks under

the guise of Salesforce employees and to be a fly on the wall in sensitive conversations with and about government customers (and the cybersecurity vulnerabilities affecting those customers, including cyber incidents discussed in this Complaint). The potential exposure of the nuances of these government cybersecurity vulnerabilities creates an imminent threat that a possible malicious actor can (and may already have) used information about government cybersecurity vulnerabilities to launch sophisticated attacks to exploit those vulnerabilities.

339. Specifically, Salesforce’s knowing violations of Government Cybersecurity Requirements created a cyber threat that allowed malicious actors to observe—undetected—Salesforce’s incident webinars with government customers.

340. To mollify its customers after serious cyber incidents, Salesforce hosts dog and pony shows billed as incident webinars. Organized by CIC, these webinars are supposed to notify customers about security incidents, including the scope of “[c]ustomer impact” from the incident, the “[p]rognosis for resolution,” the “details of root cause,” and the preventative actions to help contain the potential breach. Salesforce also represented that incident webinars would be hosted within 1-2 hours after CSIRT escalated a security incident to maximum severity or Sev0.

341. In fact, Salesforce directed its employees to limit the information provided to customers at incident webinars:

- avoid the term “[o]utage”
- instead use “service disruption”
- “[n]ever offer information about whether an employee caused the incident or whether any disciplinary action was or will be taken.”

342. Even the whitewashing of cyber incidents aside, customer incident webinars still allowed Salesforce to engage with government customers about serious, and sensitive, vulnerabilities affecting their government data. The information shared on these webinars—the nuances of cybersecurity vulnerabilities that potentially exposed government data—is a goldmine for possible malicious actors looking to further exploit those vulnerabilities.

343. At least as early as September 2021, Salesforce’s knowing violations of the Government Cybersecurity Requirements, freely invited possible malicious actors to be a fly on the wall in customer incident webinars and, worse, to do so cloaked as an authorized Salesforce employee. For example, Salesforce hosted customer webinars in April 2022 regarding the “Salesforce Heroku Cloud Incident.” On information and belief, this customer webinar was related to the Cyber Incident #13 breach alleged in this Complaint,

and the customer webinar would have relayed sensitive information that customer authentication tokens were stolen.

344. On May 11, 2021, Salesforce experienced a service disruption. The “May 11 DNS Sev0” incident was a serious service disruption that caused a blackout of all Salesforce products and that created a “wide range of impact that [was] being seen across the Salesforce environment.”

345. Salesforce gave this service disruption the code name “GRACEFUL HALL” because, while not itself a cyber incident, it caused a major business interruption for hundreds of customers, including government agencies, and was so significant that Salesforce assigned it maximum severity (Sev0). Outsiders to Salesforce described this disruption as a Salesforce “screw-up,” requiring significant outreach and attention to customers who were rightfully concerned.

346. In September 2021, Salesforce transitioned its customer incident webinars from WebEx to Zoom. This transition—which allowed 50,000 customers to attend the same customer incident webinar simultaneously—was “a key action item out of our Graceful Hall (May 11 DNS [Domain Name System] Sev0) work” in order to “provide a much-improved experience for [Salesforce] customers.”

347. Yet as with other Salesforce cyber incidents alleged in this Complaint, Salesforce was wholly unprepared to address this massive interruption to service or

respond to customers because it was “significantly below the current demand for [its] services” due to “record high incident volume,” compounding existing vulnerabilities for hackers and creating new vulnerabilities.

348. In transitioning tens of thousands of its customers to the Zoom platform for webinars, Salesforce focused on expediency over cybersecurity—and in doing so, knowingly triggered a cyber threat through Zoom by:

- licensing only four administrative Zoom accounts for sharing among dozens of Salesforce employees worldwide (“Since these are shared accounts, anyone with access could change an existing/scheduled webinar including deleting it. . . . There would be no way to audit at an individual level who made the change” and no “path to mitigate” this risk.)
- sharing passwords and usernames that were not encrypted
- sharing login credentials among at least 16 CIC employees and Salesforce global leaders responsible for setting up account user webinars with hundreds of Salesforce staff eventually having access to shared Zoom accounts
- allowing the 16 employees to share the passwords with hundreds of other team members to assist with the webinars

- failing to require Salesforce staff to routinely change passwords—compounding the cyber threat resulting from the sharing of the login credentials—thereby allowing open access to the Zoom accounts by anyone with the historical login information, including former Salesforce employees, and anyone else who may have obtained the log in credentials, e.g., due to a Google Doc having been left open
- sharing exposed unencrypted, plain text login credentials via shared documents like Google Sheets and Google Documents, and in Slack messages
- exposing Salesforce login credentials by naming (or titling) documents, “Webinar Creds” and “Zoom Password Info,” among others, outside of a “short term ask for those in this [shared] document to keep these credentials private.”
- on the flip side, obfuscating the identity of Salesforce employee users by switching their usernames from their real names to generic usernames, thereby allowing anonymous access (“We can’t have customers receive the invite from [] Dev...we a [*sic*] billion dollar company, this is not professional”)

- directing Salesforce staff to circumvent authentication requirements by logging into the Zoom account through a browser rather than a secure platform such as Single Sign-on, which allows users to log in to multiple applications with one set of credentials, or Google, “as this can prompt an OAuth flow [to authenticate] depending on which email address is entered.”
- allowing (and in fact, directing) users to login without the required multifactor authentication, thereby opening the door for an unauthorized person to access government data without detection.

349. Salesforce’s minimally reckless rollout of the Zoom platform for incident webinars was more about controlling the narrative surrounding the outage (GRACEFUL HALL) to minimize harm to its business reputation than compliance with Government Cybersecurity Requirements. This is demonstrated by the fact that Salesforce was violating even its own internal cybersecurity policies in conducting these incident webinars.

350. Further, Salesforce enabled hundreds of its employees who were designated to assist with the webinars to have anonymous access to only four administrative accounts—all using one of the four account login credentials. In

doing so, this allowed Salesforce employees (or possible malicious actors with access to these login credentials through the improper sharing of passwords) to have widespread access to government employees' PII, including their names, affiliated agencies, and email addresses for those who logged in to incident webinars.

351. In this way, Salesforce enabled possible malicious actors to covertly join these Zoom webinars as administrators to learn about GovCloud cybersecurity incidents, including questions asked by GovCloud customers about specific vulnerabilities they were experiencing and Salesforce's responses. Armed with this information, possible malicious actors could launch sophisticated attacks on government customers based on the roadmap of the cybersecurity vulnerability at issue.

352. Any cyber attack by a malicious actor through this route would be a cloaked attack; they would have learned about GovCloud vulnerabilities disguised as an authorized Salesforce employee (using one of the shared Salesforce accounts), without anyone knowing who they were or what their intentions were.

353. Salesforce was deliberate in its decision to allow credential-sharing, at one point asking itself: "do we share all accounts globally or keep the account access to PAD team and CIC multi team + CIC directors?"

354. Salesforce knew that having its staff share credentials:

- “is a severe violation of [Salesforce internal policy] SFSS-141. . . . It destroys nonrepudiation and is particularly severe if the account has any elevated privilege [like an administrative account].”
- “violates Salesforce security policy 141 . . . and because of the nature of our work, we are governed by additional security policies re: incidents and gov cloud.”
- “sharing passwords via a doc is a violation of SFSS-141.”
- Although “while this has been a known risk from the beginning, BT is investigating helping CIC set-up a shared vault to encrypt credentials.”
- “increased risk [because] We’re password sharing.”

355. Salesforce further understood that allowing its employees to use credentials that cloaked their identities violated Salesforce written policies designed to comply with Government Cybersecurity Requirements: “There should absolutely not be shared admin accounts. Nonrepudiation is destroyed if we cant [*sic*] tell who is doing what.”

356. The Salesforce CIC also knowingly failed to submit a Zoom transition plan to Information Security or seek that office’s approval to share Zoom credentials. In fact, in response to these serious concerns raised within CIC, the

CIC Senior Director directed his teams to continue credentials-sharing: “lets [*sic*] collectively make this decision between [CIC teams],” without the knowledge of Information Security.

357. Salesforce knowingly failed to comply with Government Cybersecurity Requirements and its own internal policies related to identity management, access controls, and authentication or multi-factor authentication, i.e., verifying a user’s identity as a prerequisite to their accessing data through passwords, physical authenticators, and/or biometrics. 48 C.F.R. § 52.204-21(b)(1)(v), (vi) (FAR Safeguarding Requirements)

358. Salesforce’s knowing violations of Government Cybersecurity Requirements and its own internal security policies create an imminent threat whereby possible malicious actors can gain unauthorized access not only to government users’ PII, but also to information about GovCloud vulnerabilities that permit them to launch sophisticated cyber attacks. Possible malicious actors could already have this information, because Salesforce knowingly failed to authenticate users; connect users to actions taken on their behalf; maintain confidentiality of login credentials; rotate passwords; and generally ensure basic, commonsense protections that an ordinary consumer would take to guard against theft of Salesforce login credentials and sensitive data.

359. At a company of Salesforce's size—with over 73,000 employees—these basic failures to ensure login credentials are used only by authorized employees creates the possibility of numerous cloaked attacks disguised as Salesforce employees.

360. The gravity of these cloaked attacks becomes even more paramount in light of Salesforce's recent addition of cloud storage for classified government information to its suite of offerings. Salesforce's knowing violations of even the most basic cybersecurity requirements jeopardizes government data, including the most sensitive and classified.

361. Salesforce knowingly failed to identify, protect against, detect, respond to, and recover from this self-inflicted cyber threat in violation of Government Cybersecurity Requirements, exposing sensitive government data to possible malicious actors and creating an imminent threat that possible malicious actors will exploit cybersecurity vulnerabilities and harm government agencies and national security. [48 C.F.R. § 52.204-21](#) (FAR Safeguarding Requirements); [48 C.F.R. § 252.204-7012](#) (DFARS 7012)

362. Because of these persistent and unabated violations of Government Cybersecurity Requirements, Salesforce knowingly submitted false or fraudulent claims to government agencies and submitted false records material to fraudulent claims; and the government agencies paid those claims.

V. MATERIALITY

363. Salesforce knew that compliance with the Government Cybersecurity Requirements was material to the government's decision to pay claims under the contracts for cloud services and products. Salesforce also knew that truthful records and statements in support of claims under the government contracts were material to the government's decision to pay these claims.

364. Some of the factors in evaluating materiality under the False Claims Act include (a) statutory, regulatory, and contractual language, (b) whether the violations go to the heart of the benefit of the bargain, (c) whether the violations were serious and material and not merely technical or minor infractions of rules, (d) the government's actions relative to similar violations, (e) whether any reasonable person would attach importance to Defendant's choice of actions, and (f) Defendant's knowledge relative to these factors. All these factors demonstrate materiality in this case and have been addressed throughout this Complaint.

365. Salesforce knowingly submitted or caused to be submitted thousands of false or fraudulent claims and used false records and statements in support of false or fraudulent claims under government contracts in violation of the Government Cybersecurity Requirements designed to safeguard sensitive government data. In turn, the government paid those claims.

366. This case is precisely the type of fraud scheme remedied by the False Claims Act. One example is *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings*:

These acquisition regulations require that the defense contractor undertake cybersecurity specific measures before the contractor can handle certain technical information. Here, compliance with these cybersecurity requirements could have affected AR's ability to handle technical information pertaining to missile defense and rocket engine technology. Accordingly, misrepresentations as to compliance with these cybersecurity requirements could have influenced the extent to which AR could have performed the work specified by the contract. (internal citations omitted)

U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., Memorandum and Order Re: Defendants' Motion to Dismiss, [381 F. Supp. 3d 1240, 1248](#) (E.D. Cal. 2019).

367. In July 2022, after the summary judgment decision in favor of plaintiff, Aerojet Rocketdyne agreed to pay \$9 million to resolve allegations by a former employee that Aerojet violated cybersecurity requirements in federal government contracts, including with DOD and NASA. Press Release, *Aerojet Rocketdyne Agrees to Pay \$9 Million to Resolve False Claims Act Allegations of*

Cybersecurity Violations in Federal Government Contracts (July 8, 2022), <https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity>

368. In speaking about the Aerojet settlement, DOJ Principal Deputy Assistant Attorney General Brian M. Boynton recognized that “[w]histleblowers with inside information and technical expertise can provide crucial assistance in identifying knowing cybersecurity failures and misconduct.” Press Release, *Aerojet Rocketdyne Agrees to Pay \$9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts* (July 8, 2022), <https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity>

369. The United States also filed a “statement of interest” supporting the plaintiff’s summary judgment briefing that led to a favorable decision for the plaintiff. *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Memorandum and Order Re: Cross Motions for Summary Judgment, No. 2:15-cv-02245 WBS AC, [2022 WL 297093](https://www.courtlistener.com/doc/2022/02/01/2022-WL-297093) (E.D. Cal. Feb. 1, 2022) (slip op.); United States’ Statement of Interest in Connection with Defendants’ Summary Judgment Motion, *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245 (Oct. 20, 2021), <https://www.onlineandonpoint.com/wp-content/uploads/sites/40/2022/02/Aerojet-Statement-of-Interest.pdf>

370. In denying the defendants’ motion for summary judgment, the Court found that “[i]t may be reasonably inferred that compliance [with FAR clauses mandating cybersecurity protections] was significant to the government because without complete knowledge about compliance, or noncompliance, with the clauses, the government cannot adequately protect its information.” *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Memorandum and Order Re: Cross Motions for Summary Judgment, No. 2:15-cv-02245 WBS AC, [2022 WL 297093](#), at *7 (E.D. Cal. Feb. 1, 2022) (slip op.).

371. In a different case, in March 2022, a medical services contractor agreed to pay nearly \$1 million to resolve allegations that it falsely represented to the U.S. State Department and the U.S. Air Force that it would use a secure electronic medical records system in providing medical services to U.S. military service members, diplomats, officials, and contractors working in certain conflict zones, to protect the confidentiality of their health information and PII. The contractor’s failure to utilize a secure system exposed sensitive medical records and PII to non-clinical staff. Again, the DOJ Principal Deputy Assistant General stated, “This settlement demonstrates the department’s commitment to use its civil enforcement tools to pursue government contractors that fail to follow required cybersecurity standards . . . We will continue to ensure that those who do business with the government comply with their contractual obligations, including those

requiring the protection of sensitive government information.” Press Release, *Medical Services Contractor Pays \$930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts in State Department and Air Force Facilities in Iraq and Afghanistan* (Mar. 8, 2022), <https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical>

372. Further, in July 2019, a contractor agreed to pay \$8.6 million to resolve allegations that it knowingly sold flawed video surveillance systems to federal and state government entities that *may* have but did not actually result in the disclosure of information. Press Release, *Attorney General James Secures \$6 Million from Cisco Systems in Multistate Settlement* (Aug. 1, 2019), <https://ag.ny.gov/press-release/2019/attorney-general-james-secures-6-million-cisco-systems-multistate-settlement>; *Cisco to Pay \$8.6 Million to Settle Government Claims of Flawed Tech*, N.Y. TIMES (July 31, 2019), <https://www.nytimes.com/2019/07/31/technology/cisco-tech-flaw-sales.html>

373. In an earlier case, in November 2015, a contractor and subcontractor responsible for implementing software to manage the DOD’s telecommunications network collectively agreed to pay \$12.75 million to resolve allegations that they allowed unauthorized access to sensitive government data by using individuals on the contract who lacked the requisite security clearances. Press Release,

Netcracker Technology Corp. and Computer Sciences Corp. Agree to Settle Civil False Claims Act Allegations (Nov. 2, 2015),

<https://www.justice.gov/opa/pr/netcracker-technology-corp-and-computer-sciences-corp-agree-settle-civil-false-claims-act>

374. In a recent memorandum, the DOD reiterated that failure to adhere to the DFARS 7012 mandate or make progress on a plan to comply with NIST-171 may be “a material breach of contract requirements. Remedies for such a breach may include withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole.” This demonstrates that compliance with DFARS 7012 and NIST-171 is material to the government’s decision to pay claims under contracts.

375. DOJ in partnership with federal agencies has also made cybersecurity fraud an enforcement priority. The Deputy Attorney General (DAG) unveiled DOJ’s False Claims Act Cyber-Fraud Initiative to pursue cybersecurity related fraud by government contractors, including the fraud scheme alleged here, to “hold accountable entities or individuals that put U.S. information or systems at risk” by:

- “knowingly providing deficient cybersecurity products or services,”
- “knowingly misrepresenting their cybersecurity practices or protocols,” or

- “knowingly violating obligations to monitor and report cybersecurity incidents and breaches.”

Press Release, Office of Public Affairs, U.S. Department of Justice, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>; and Remarks of Brian Boynton, Acting Assistant Attorney General, Civil Division, U.S. Department of Justice (Oct. 13, 2021), <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

376. The facts alleged in this Complaint show that Salesforce was well aware that the Government Cybersecurity Requirements, and compliance with government security alerts, advisories, and directives, were “essential” to the government’s decision to pay claims because of the “critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.” NIST-53 at SI-5 Control and Discussion, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

377. Salesforce also knew that the unlawful conduct alleged in this Complaint went to the very heart of the bargain for the payment of claims under

the contracts for cybersecurity services. The government expects and requires that claims be paid only for accurate and truthful claims under government contracts.

378. Salesforce's statutory and programmatic requirements for complete, accurate, and truthful reporting during the claims' submission process under the government contracts go directly to the "essence of the bargain." These requirements are neither "minor nor insubstantial."

379. Salesforce's violations of the statutory, regulatory, and contractual requirements were serious and material, leading to actual or potential harm, and were made with at least reckless disregard of the seriousness of their violations.

380. Salesforce's violations were not immaterial or inadvertent technical mistakes in processing paperwork, or simple and honest misunderstanding of the rules, terms and conditions, or certification requirements. Rather, Salesforce knowingly failed to comply with material legal obligations and certifications.

381. Salesforce knew that it was submitting or causing to submit false or fraudulent claims and false or fraudulent statements and records in support of false claims, which the government paid.

382. In short, there is ample evidence to show that Salesforce knew or should have known that its violations had the natural tendency to influence the government's decision to pay the claims under government contracts and that any reasonable person would attach importance to its choice of action.

VI. UNLAWFUL RETALIATION

383. Relator was employed at Salesforce as a Senior Manager, Critical Incident Center, from January 31, 2020, to May 2, 2022. While at Salesforce, Relator was troubled that Defendant was engaged in unlawful practices alleged in this Complaint. Relator also feared job security and the legal propriety of Defendant's actions. Relator repeatedly and consistently informed management of concerns related directly to the allegations set forth in the Complaint.

384. Yet Relator was continually ignored, reprimanded, marginalized, belittled, discriminated against in terms of the conditions of employment, and constructively discharged, for raising concerns related to, and objecting to, Defendant's fraudulent course of conduct alleged in this Complaint.

385. Defendant retaliated against and constructively discharged Relator because of lawful acts by Relator to stop one or more violations of the False Claim Act and lawful acts by Relator in furtherance of an action under 31 U.S.C. § 3730.

386. Below are some specific events that occurred, which are relevant to the retaliation allegations in this Complaint.

387. Starting in June 2021 and over the next several months, Relator raised with CIC management cybersecurity concerns related to Salesforce's use of the Zoom platform alleged in this Complaint but was dismissed, ignored, and denied multiple requests to involve the Information Security department.

388. As Relator and his team became increasingly concerned, in early September 2021, Relator escalated his concerns by filing a ticket with Information Security and was informed that his concerns were in fact valid and revealed a violation of internal security policy.

389. In response, in September 2021, Relator was directed to the internal EthicsPoint system and once again escalated his concerns internally by filing a policy violation report.

390. In September 2021, Salesforce added two new CIC leaders for the U.S. (or AMER) team leads, demoting Relator in responsibility from being the sole U.S. lead, to one of three leads, thereby greatly diminishing Relator's influence, impact, and responsibility.

391. Shortly thereafter, in a one-on-one meeting with CIC management, Relator was told that he was no longer considered a "team player", that pursuing his concerns had a significant "impact" on his "personal brand," and that Salesforce brought in more leads to help protect his brand.

392. Despite the escalation of Relator's concerns, Relator continued to be dismissed by management and was informed that his career would be negatively impacted as a result of him reporting and acting on his concerns.

393. In October 2021, Relator again escalated his concerns by filing a formal complaint with Salesforce's Senior Manager for Employee Relations.

394. In December 2021, Relator applied for a new role within the organization. In February 2022, Relator was informed that the hiring team would not be moving forward with his candidacy.

395. That same month, in February 2022, Relator raised concerns about retaliation through a Concierge ticket.

396. In March 2022, in an additional one-on-one meeting with CIC management, Relator was informed that he would be further demoted and no longer a people manager at the organization. Because of this hostile work environment, Relator was constructively discharged and left Salesforce on May 2, 2022.

397. For the reasons set forth in this Complaint, Relator is entitled to double the amount of back pay, interest on the back pay and compensation for any special damages sustained as a result of the retaliation, including litigation costs and reasonable attorneys' fees, and all other remedies and recompense allowable under 31 U.S.C. § 3730(h) and the various states' retaliation provisions alleged in this Complaint.

VII. COUNTS

COUNT I

**Federal False Claims Act:
31 U.S.C. § 3729(a)(1)(A)**

398. The allegations in the preceding paragraphs are incorporated by reference.

399. Defendant knowingly presented or caused to be presented false or fraudulent claims for payment or approval in violation of 31 U.S.C. § 3729(a)(1)(A).

400. The United States paid for claims that otherwise would not have been allowed.

401. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

402. As a result of these violations, the United States has suffered damages in an amount to be determined at trial.

COUNT II

Federal False Claims Act: 31 U.S.C. § 3729(a)(1)(B)

403. The allegations in the preceding paragraphs are incorporated by reference.

404. Defendant knowingly made, used or caused to be made or used, false records or statements material to false or fraudulent claims, in violation of 31 U.S.C. § 3729 (a)(1)(B).

405. The United States paid for claims that otherwise would not have been allowed.

406. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

407. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

COUNT III

**Federal False Claims Act:
31 U.S.C. § 3729(a)(1)(C)
Conspiracy**

408. The allegations in the preceding paragraphs are incorporated by reference.

409. Defendant knowingly conspired to commit a violation of the False Claims Act, in violation of 31 U.S.C. § 3729 (a)(1)(C).

410. The United States paid for claims that otherwise would not have been allowed.

411. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus

civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

412. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

COUNT IV

**Federal False Claims Act:
31 U.S.C. § 3729(a)(1)(G)**

413. The allegations in the preceding paragraphs are incorporated by reference.

414. Defendant knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money or property to the Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money or property to the Government, in violation of 31 U.S.C. § 3729 (a)(1)(G).

415. The United States paid for claims that otherwise would not have been allowed.

416. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

417. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

COUNT V

Retaliation of Relator in Violation of False Claims Act 31 U.S.C. § 3730(h)

418. The allegations in the preceding paragraphs are incorporated by reference.

419. Relator engaged in lawful acts in furtherance of efforts to stop one or more violations of 31 U.S.C. § 3729.

420. Because of Relator's lawful acts, Relator was subjected to retaliation by Defendant.

421. Relator was unlawfully retaliated against by Defendant and for engaging in protected activity, namely for raising, objecting to and refusing to participate in fraudulent conduct alleged in this Complaint.

422. Defendant's retaliation against Relator was a violation of 31 U.S.C. § 3730(h).

423. As a consequence of Defendant's violations of 31 U.S.C. § 3730(h), Relator suffered damages.

424. Relator is entitled to damages sustained as a result of the retaliation, including litigation costs and reasonable attorneys' fees, and all other remedies and recompense allowable under 31 U.S.C. § 3729(h).

425. As a direct and proximate result of Defendant's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under 31 U.S.C. § 3729(h).

COUNT VI

California False Claims Act, Cal. Gov't Code § 12650, et seq.

426. The allegations in the preceding paragraphs are incorporated by reference.

427. Relator also brings this action on behalf of the State of California, against Defendant under the California False Claims Act ("FCA"), Cal. Gov't Code § 12652(c).

428. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the California FCA, Cal. Gov't Code § 12651(a)(1), which creates liability for any person who "[k]nowingly presents or causes to be presented a false or fraudulent claim for payment or approval."

429. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the California FCA, Cal. Gov't Code § 12651(a)(2), which creates liability for any person who "[k]nowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim."

430. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the California FCA, Cal. Gov't Code § 12651(a)(3), which creates liability for any person who “conspires to commit a violation of this subdivision.”

431. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the California FCA, Cal. Gov't Code § 12651(a)(7), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used a false record or statement material to an obligation to pay or transmit money or property to the state or to any political subdivision, or knowingly conceals or knowingly and improperly avoids, or decreases an obligation to pay or transmit money or property to the state or to any political subdivision.”

432. Pursuant to the California FCA, based on Defendant's material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Cal. Gov't Code § 12651(a).

433. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT VII

Unlawful Retaliation Under California False Claims Act Cal. Gov. Code § 12650, et seq.

434. The allegations in the preceding paragraphs are incorporated by reference.

435. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

436. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of Cal. Gov. Code § 12651, unlawfully retaliated against Relator.

437. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all relief allowable under Cal. Gov. Code § 12653.

COUNT VIII

District of Columbia False Claims Act, D.C. Code Ann. §§ 2.381.01, et seq.

438. The allegations in the preceding paragraphs are incorporated by reference.

439. Relator also brings this action in the name of the District of Columbia, against Defendant under the District of Columbia False Claims Act, D.C. Code Ann. § 2-381.03(b)(1).

440. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the D.C. FCA, D.C. Code Ann. § 2-381.02(a)(1), which creates liability for any person who “[k]nowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval.”

441. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the D.C. FCA, D.C. Code Ann. § 2-381.02(a)(2), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim.”

442. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the D.C. FCA, D.C. Code Ann. § 2-381.02(a)(6), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the District, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the District.”

443. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the

D.C. FCA, D.C. Code Ann. § 2-381.02(a)(7), which creates liability for any person who “conspires to commit a violation” of certain provisions of this subsection.

444. Pursuant to the D.C. FCA, based on Defendant’s material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Defendant is thus liable to the District for statutorily defined damages sustained because of the acts of Defendant and civil penalties. D.C. Code Ann. § 2-381.02(a).

445. As a result of Defendant’s violations, the District has suffered damages in an amount to be determined at trial.

COUNT IX

Unlawful Retaliation Under District of Columbia False Claims Act DC ST § 2-381.01, *et seq.*

446. The allegations in the preceding paragraphs are incorporated by reference.

447. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

448. Salesforce, with actual knowledge of Relator’s lawful acts in furtherance of this action and efforts to stop Defendant’s violations of DC ST § 2-381.02, unlawfully retaliated against Relator.

449. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under DC ST § 2-381.04.

COUNT X

Delaware False Claims & Reporting Act, Del. Code Ann. Tit. 6 § 1201, et seq.

450. The allegations in the preceding paragraphs are incorporated by reference.

451. Relator also brings this action on behalf of the Government of the State of Delaware, against Defendant under the State of Delaware's False Claims and Reporting Act ("FCA"), Del. Code Ann. tit. 6, §§ 1201(a) and 1203(b)(1).

452. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Delaware FCA, Del. Code Ann. tit. 6, §1201(a)(1), which creates liability for any person who "[k]nowingly presents or causes to be presented a false or fraudulent claim for payment or approval."

453. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Delaware FCA, Del. Code Ann. tit. 6, §1201(a)(2), which creates liability for any person who "[k]nowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim."

454. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Delaware FCA, Del. Code Ann. tit. 6, §1201(a)(3), which creates liability for any person who “conspires to commit a violation of” certain provisions in this section.

455. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Delaware FCA, Del. Code Ann. tit. 6, §1201(a)(7), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government.”

456. Pursuant to the Delaware FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Del. Code Ann. tit. 6, §1201(a).

457. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XI

Unlawful Retaliation Under Delaware False Claims & Reporting Act 6 Del. Code §§ 1201-1211

458. The allegations in the preceding paragraphs are incorporated by reference.

459. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

460. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of 6 Del. Code § 1201, unlawfully retaliated against Relator.

461. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under 6 Del. Code § 1208(a) and (b).

COUNT XII

Florida False Claims Act, Fla. Stat. § 68.081, *et seq.*

462. The allegations in the preceding paragraphs are incorporated by reference.

463. Relator also brings this action on behalf of the State of Florida, against Defendant under the State of Florida's False Claims Act ("FCA"), Fla. Stat. Ann. §§ 68.082(2) and § 68.083(2).

464. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Florida FCA, Fla.

Stat. Ann. § 68.082(2)(a), which creates liability for any person who “[k]nowingly presents or causes to be presented a false or fraudulent claim for payment or approval.”

465. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Florida FCA, Fla. Stat. Ann. § 68.082(2)(b), creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim.”

466. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Florida FCA, Fla. Stat. Ann. § 68.082(2)(c), creates liability for any person who “conspires to commit a violation of this subsection.”

467. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Florida FCA, Fla. Stat. Ann. § 68.082(2)(g), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used a false record or statement material to an obligation to pay or transmit money or property to the state, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the state.”

468. Pursuant to the Florida FCA, based on Defendant's material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. [Fla. Stat. Ann. § 68.082\(2\)](#).

469. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT XIII

Unlawful Retaliation Under Florida False Claims Act [Fla. Stat. §§ 68.081-68.092](#)

470. The allegations in the preceding paragraphs are incorporated by reference.

471. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

472. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action, unlawfully retaliated against Relator.

473. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under [Fla. Stat. §§ 68.088](#) and [112.3187\(9\)](#).

COUNT XIV

Hawaii False Claims Act,

Haw. Rev. Stat. §§ 661-21, et seq.

474. The allegations in the preceding paragraphs are incorporated by reference.

475. Relator also brings this action on behalf of the State of Hawaii and its political subdivisions, against Defendant under the Hawaii False Claims Act, Haw. Rev. Stat. §§ 661-21(a) and 661-25(a).

476. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the Hawaii FCA, Haw. Rev. Stat. § 661-21(a)(1), which creates liability for any person who “[k]nowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval.”

477. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the Hawaii FCA, Haw. Rev. Stat. § 661-21(a)(2), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim.”

478. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the Hawaii FCA, Haw. Rev. Stat. § 661-21(a)(6), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used, a false record or

statement material to an obligation to pay or transmit money or property to the State, or knowingly conceals, or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the State.”

479. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated the provision of the Hawaii FCA, Haw. Rev. Stat. § 661-21(a)(8), which creates liability for any person “conspires to commit any of the conduct described in this subsection.”

480. Pursuant to the Hawaii FCA, based on Defendant’s material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Haw. Rev. Stat. § 661-21(a).

481. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XV

Unlawful Retaliation Under Hawaii False Claims Act Haw. Rev. Stat. § 661-21, et seq.

482. The allegations in the preceding paragraphs are incorporated by reference.

483. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

484. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of Haw. Rev. Stat. § 661-21, unlawfully retaliated against Relator.

485. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under H.R.S. § 661-30(a) and (b).

COUNT XVI

Illinois False Claims Act, 740 Ill. Comp. Stat. 175/1, et seq.

486. The allegations in the preceding paragraphs are incorporated by reference.

487. Relator also brings this action on behalf of the State of Illinois, against Defendant under the Illinois False Claims Act ("FCA"), 740 Ill. Comp. Stat. §§ 175/3(a) and 175/4(b).

488. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Illinois FCA, 740 Ill. Comp. Stat. 175/3(a)(1)(A), which creates liability for any person who "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval."

489. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Illinois FCA, 740

Ill. Comp. Stat. 175/3(a)(1)(B), which creates liability for any person who “knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim.”

490. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Illinois FCA, 740 Ill. Comp. Stat. 175/3(a)(1)(C), which creates liability for any person who “conspires to commit a violation” of certain subparagraphs in this section.

491. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Illinois FCA, 740 Ill. Comp. Stat. 175/3(a)(1)(G), which creates liability for any person who “knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the State, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the State.”

492. Pursuant to the Illinois FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. 740 Ill. Comp. Stat. 175/3(a).

493. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XVII

Unlawful Retaliation Under Illinois False Claims Act 740 ILCS §§ 175/1 to 175/8

494. The allegations in the preceding paragraphs are incorporated by reference.

495. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

496. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of 740 ILCS §§ 175/3, unlawfully retaliated against Relator.

497. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under 740 ILCS 175/4(g)(1) and (2).

COUNT XVIII

Indiana False Claims and Whistleblower Protection Act Ind. Code Ann. § 5-11-5.5-1, *et seq.*

498. The allegations in the preceding paragraphs are incorporated by reference.

499. Relator also brings this action on behalf of the State of Indiana, against Defendant under the State of Indiana False Claims and Whistleblower Protection Act (“FCA”), Ind. Code Ann. §§ 5-11-5.5-2(b) and 5-11-5.5-4(a).

500. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Indiana FCA, Ind. Code § 5-11-5.5-2(b)(1), creates liability for any person who “knowingly or intentionally presents a false claim to the state for payment or approval.”

501. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Indiana FCA, Ind. Code § 5-11-5.5-2(b)(2), creates liability for any person who “knowingly or intentionally makes or uses a false record or statement to obtain payment or approval of a false claim from the state.”

502. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Indiana FCA, Ind. Code § 5-11-5.5-2(b)(6), which creates liability for any person who “knowingly or intentionally made or used a false record or statement to avoid an obligation to pay or transmit property to the State of Indiana.”

503. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Indiana FCA, Ind.

Code § 5-11-5.5-2(b)(7), which creates liability for any person who “conspires with another person to perform an act described” in certain subdivisions.

504. Pursuant to the Indiana FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Ind. Code §§ 5-11-5.5-2(b) and 5-11-5.5-4(a).

505. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XIX

Unlawful Retaliation Under Indiana False Claims and Whistleblower Protection Act Ind. Code Ann. §§ 5-11-5.5-1 - 5-11-5.5-18

506. The allegations in the preceding paragraphs are incorporated by reference.

507. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

508. Salesforce, with actual knowledge of Relator’s lawful acts in furtherance of this action and other efforts to stop Defendant’s violations of Ind. Code Ann. § 5-11-5.5-2, unlawfully retaliated against Relator.

509. As a direct and proximate result of Salesforce’s retaliatory actions, Relator suffered damages and is entitled to all allowable relief under Ind. Code Ann. § 5-11-5.5-8.

COUNT XX

Iowa False Claims Act, Iowa Code Ann. § 685, et seq.

510. The allegations in the preceding paragraphs are incorporated by reference.

511. Relator also brings this action on behalf of the State of Iowa, against Defendant under the State of Iowa False Claims Act (“FCA”), Iowa Code Ann. §§ 685.2(1), 685.3(2)a.

512. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Iowa FCA, Iowa Code Ann. § 685.2(1)(a), which creates liability for any person who “[k]nowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval.”

513. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Iowa FCA, Iowa Code Ann. § 685.2(1)(b), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim.”

514. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Iowa FCA, Iowa Code Ann. § 685.2(1)(c), which creates liability for any person who “conspires to commit a violation of” certain paragraphs in this section.

515. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Iowa FCA, Iowa Code Ann. § 685.2(1)(g), which creates liability for any person who “[k]nowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the state, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the state.”

516. Pursuant to the Iowa FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Iowa Code Ann. §§ 685.2(1), 685.3(2)a.

517. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXI

Unlawful Retaliation Under Iowa False Claims Act IA Code Ann. §§ 685.1 through 685.7

518. The allegations in the preceding paragraphs are incorporated by reference.

519. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

520. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of IA Code Ann. § 685.2, unlawfully retaliated against Relator.

521. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under IA Code Ann. §§ 685.3(6)(a) and (b).

COUNT XXII

The Commonwealth of Massachusetts False Claims Act, Mass. Ann. Laws Ch. 12, § 5A-50

522. The allegations in the preceding paragraphs are incorporated by reference.

523. Relator also brings this action on behalf of the Commonwealth of Massachusetts, against Defendant under the Massachusetts False Claims Act ("FCA"), Mass. Ann. Laws ch. 12, §§ 5B and 5C(2).

524. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Massachusetts

FCA, Mass. Ann. Laws ch. 12, § 5B(1), which creates liability for any person who “knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval.”

525. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Massachusetts FCA, Mass. Ann. Laws ch. 12, § 5B(2), creates liability for any person who “knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim.”

526. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Massachusetts FCA, Mass. Ann. Laws ch. 12, § 5B(3), creates liability for any person who “conspires to commit a violation of this subsection.”

527. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated the provision of the Massachusetts FCA, Mass. Ann. Laws ch. 12, § 5B(9), which creates liability for any person who “knowingly makes, uses or causes to be made or used a false record or statement material to an obligation to pay or to transmit money or property to the commonwealth or a political subdivision thereof, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the commonwealth or a political subdivision thereof.”

528. Pursuant to the Massachusetts FCA, based on Defendant's material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Mass. Ann. Laws ch. 12, § 5B.

529. As a result of Defendant's violations, the Commonwealth has suffered damages in an amount to be determined at trial.

COUNT XXIII

Unlawful Retaliation Under Massachusetts False Claims Act Mass. Ann. Laws Ch. 12, §§ 5A- 5O

530. The allegations in the preceding paragraphs are incorporated by reference.

531. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

532. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of M.G.L.A. 12 § 5B to 5O, unlawfully retaliated against Relator.

533. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under M.G.L.A. 12 § 5J.

COUNT XXIV

Minnesota False Claims Act, Minn. Stat. §§ 15C.01, et seq.

534. The allegations in the preceding paragraphs are incorporated by reference.

535. Relator also brings this action on behalf of the State of Minnesota and its political subdivisions, against Defendant under the State of Minnesota False Claims Act, Minn. Stat. § 15C.05(a).

536. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated each of the following provisions of the Minnesota FCA, Minn. Stat. § 15C.02(a), which create liability for any person who:

- “(1) knowingly presents, or causes to be presented, to an officer or employee of the state or a political subdivision a false or fraudulent claim for payment or approval;
- (2) knowingly makes or uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the state or a political subdivision;
- (3) knowingly conspires to either present a false or fraudulent claim to the state or a political subdivision for payment or approval or makes,

uses, or causes to be made or used a false record or statement to obtain payment or approval of a false or fraudulent claim; [or]

...

- (7) knowingly makes or uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the state or a political subdivision.”

537. Pursuant to the Minnesota FCA, based on Defendant’s material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Minn. Stat. § 15C.01 et seq.

538. As a result of Defendant’s violations, the state has suffered damages in an amount to be determined at trial.

COUNT XXV

Unlawful Retaliation Under Minnesota False Claims Act M.S.A. § 15C.01, *et seq.*

539. The allegations in the preceding paragraphs are incorporated by reference.

540. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

541. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of M.S.A. § 15C.02, unlawfully retaliated against Relator.

542. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under M.S.A. § 15C.145.

COUNT XXVI

Montana False Claims Act, Mont. Code Ann. § 17-8-401, et seq.

543. The allegations in the preceding paragraphs are incorporated by reference.

544. Relator also brings this action on behalf of the State of Montana, against Defendant under the State of Montana False Claims Act ("FCA"), Mont. Code Ann. § 17-8-406(1).

545. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the Montana FCA, Mont. Code Ann. § 17-8-403(1), which creates liability for any person who:

- “(a) knowingly presents or causes to be presented a false or fraudulent claim for payment or approval;

- (b) knowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim;
- (c) conspires to commit a violation of this subsection (1); [or]
...
- (g) knowingly makes, uses, or causes to be made or used a false record or statement material to an obligation to pay or transmit money or property to a governmental entity or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to a governmental entity.”

546. Pursuant to the Montana FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Mont. Code Ann. § 17-8-403(2).

547. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXVII

Unlawful Retaliation Under Montana False Claims Act Mont. Code Ann. §§ 17-8-401 to 17-8-416

548. The allegations in the preceding paragraphs are incorporated by reference.

549. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

550. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of Mont. Code Ann. § 17-8-403, unlawfully retaliated against Relator.

551. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under Mont. Code Ann. § 17-8-412.

COUNT XXVIII

Nevada False Claims Act, Nev. Rev. Stat. § 357.010, et seq.

552. The allegations in the preceding paragraphs are incorporated by reference.

553. Relator also brings this action on behalf of the State of Nevada, against Defendant under the State of Nevada Submission of False Claims to State or Local Government Act ("FCA"), Nev. Rev. Stat. § 357.080(1).

554. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the

Nevada FCA, Nev. Rev. Stat. § 357.040(1), which create liability for any person who:

- “(a) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval.
- (b) Knowingly makes or uses, or causes to be made or used, a false record or statement that is material to a false or fraudulent claim.
- ...
- (f) Knowingly makes or uses, or causes to be made or used, a false record or statement that is material to an obligation to pay or transmit money or property to the State or a political subdivision;
- (g) Knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the State or a political subdivision; or
- ...

Conspires to commit any of the acts set forth in this subsection.

555. Pursuant to the Nevada FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. Nev. Rev. Stat. § 357.040(2).

556. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXIX

Unlawful Retaliation Under Nevada False Claims Act Nev. Rev. Stat. §§ 357.010, et seq.

557. The allegations in the preceding paragraphs are incorporated by reference.

558. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

559. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and other efforts to stop Defendant's violations of Nev. Rev. Stat. § 357.040, unlawfully retaliated against Relator.

560. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under Nev. Rev. Stat. § 357.250.

COUNT XXX

New Jersey False Claims Act, N.J. Stat. Ann. § 2A:32C-1, et seq.

561. The allegations in the preceding paragraphs are incorporated by reference.

562. Relator also brings this action in the name of the State of New Jersey, against Defendant pursuant to the State of New Jersey False Claims Act (“FCA”), N.J. Stat. Ann. § 2A:32C-5.b.

563. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of The New Jersey FCA, N.J. Stat. Ann. § 2A:32C-3, which creates liability for any person who:

- “a. Knowingly presents or causes to be presented to an employee, officer or agent of the State, or to any contractor, grantee, or other recipient of State funds, a false or fraudulent claim for payment or approval;
- b. Knowingly makes, uses, or causes to be made or used a false record or statement to get a false or fraudulent claim paid or approved by the State;
- c. Conspires to defraud the State by getting a false or fraudulent claim allowed or paid by the State;
- ...
- g. Knowingly makes, uses, or causes to be made or used a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the State.”

564. Pursuant to the New Jersey FCA, based on Defendant's material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. N.J. Stat. Ann. § 2A:32C-3.

565. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXXI

Unlawful Retaliation Under New Jersey False Claims Act N.J.S.A. §§ 2A:32C-1, et seq.

566. The allegations in the preceding paragraphs are incorporated by reference.

567. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

568. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action, unlawfully retaliated against Relator.

569. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under NJSA 2A:32C-10.

COUNT XXXII

New Mexico Fraud Against Taxpayers Act,

N.M.S.A. § 44-9-1, et seq.

570. The allegations in the preceding paragraphs are incorporated by reference.

571. Relator also brings this action on behalf of the State of New Mexico, against Defendant under the New Mexico Fraud Against Taxpayers Act, N.M. N.M.S.A. §§ 44-9-3(C) and 44-9-5(A).

572. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the New Mexico Fraud Against Taxpayers Act, which create liability for any persons who:

- “(1) knowingly present, or cause to be presented, to an employee, officer or agent of the state or a political subdivision or to a contractor, grantee or other recipient of state or political subdivision funds a false or fraudulent claim for payment or approval;
- (2) knowingly make or use, or cause to be made or used, a false, misleading or fraudulent record or statement to obtain or support the approval of or the payment on a false or fraudulent claim;
- (3) conspire to defraud the state or a political subdivision by obtaining approval or payment on a false or fraudulent claim;
- (4) conspire to make, use or cause to be made or used, a false, misleading or fraudulent record or statement to conceal, avoid or decrease an

obligation to pay or transmit money or property to the state or a political subdivision;

...

- (8) knowingly make or use, or cause to be made or used, a false, misleading or fraudulent record or statement to conceal, avoid or decrease an obligation to pay or transmit money or property to the state or a political subdivision; or
- (9) as a beneficiary of an inadvertent submission of a false claim and having subsequently discovered the falsity of the claim, fail to disclose the false claim to the state or political subdivision within a reasonable time after discovery.

573. Pursuant to the New Mexico FCA, Defendant is thus liable to the State for statutorily defined damages sustained because of the acts of Defendant and such other relief as authorized. N.M. Stat. Ann. § 27-14-4.

574. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXXIII

Unlawful Retaliation Under New Mexico Fraud Against Taxpayers Act N.M.S.A. §§ 44-9-1, *et seq.*

575. The allegations in the preceding paragraphs are incorporated by reference.

576. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

577. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action, unlawfully retaliated against Relator.

578. As a direct and proximate result of Defendant's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under N.M.S.A. § 44-9-11.

COUNT XXXIV

New York False Claims Act, N.Y. State Fin. Law §§ 187, et seq.

579. The allegations in the preceding paragraphs are incorporated by reference.

580. Relator also brings this action on behalf of the State of New York, against Defendant under the State of New York False Claims Act, N.Y. State Fin. Law § 190(2).

581. Defendant, through its material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, violated each of the following provisions of the New York FCA, N.Y. State Fin. Law § 189(1), which create liability for any person who:

- “(a) knowingly presents, or causes to be presented a false or fraudulent claim for payment or approval;
- (b) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;
- (c) conspires to commit a violation of paragraph (a), (b), (d), (e), (f) or (g) of this subdivision; or
- ...
- (g) knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the state or a local government.”

582. Pursuant to the New York FCA, based on Defendant’s material misrepresentations, non-disclosures, and other wrongful acts and omissions set forth above, Defendant is liable to the State or a local government, as applicable, for treble damages, civil penalties, including consequential damages, which the state or local government sustains because of the act of the person, and all other relief authorized by law. N.Y. State Fin. Law § 189(1).

583. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXXV

Unlawful Retaliation Under New York False Claims Act State Finance Law §§ 187 et seq.

584. The allegations in the preceding paragraphs are incorporated by reference.

585. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

586. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and efforts to stop Defendant's violations of State Fin. Law § 189, unlawfully retaliated against Relator.

587. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under State Fin. Law § 191.

COUNT XXXVI

New York City False Claims Act N.Y.C. Admin Code §§ 7-801, et seq.

588. The allegations in the preceding paragraphs are incorporated by reference.

589. Relator also brings this action on behalf of New York City, against Defendant under the New York City False Claims Act ("NYC FCA"), N.Y.C. Admin Code § 7-804.

590. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the NYC FCA, N.Y.C. Admin Code § 7-803, which creates liability for any person who:

- “1. knowingly presents, or causes to be presented, to any city officer or employee, a false claim for payment or approval by the city;
2. knowingly makes, uses, or causes to be made or used, a false record or statement to get a false claim paid or approved by the city;
3. conspires to defraud the city by getting a false claim allowed or paid by the city;
- ...
7. knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease, directly or indirectly, an obligation to pay or transmit money or property to the city.”

591. Pursuant to the NYC FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the City for treble damages, civil penalties, and all other relief authorized by law. N.Y.C. Admin Code § 7-803.

592. As a result of Defendant's violations, the City has suffered damages in an amount to be determined at trial.

COUNT XXXVII

Unlawful Retaliation Under New York City False Claims Act N.Y.C. Admin Code §§ 7-801, et seq.

593. The allegations in the preceding paragraphs are incorporated by reference.

594. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

595. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and efforts to stop Defendant's violations of N.Y.C. Admin Code § 7-803, unlawfully retaliated against Relator.

596. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under N.Y.C. Admin Code § 7-805.

COUNT XXXVIII

North Carolina False Claims Act, N.C. Gen. Stat. § 1-605, et seq.

597. The allegations in the preceding paragraphs are incorporated by reference.

598. Relator also brings this action on behalf of the State of North Carolina, against Defendant under the State of North Carolina False Claims Act (“FCA”), [N.C. Gen. Stat. § 1-608\(b\)](#).

599. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the North Carolina FCA, [N.C. Gen. Stat. § 1-607\(a\)](#), which creates liability for any person who:

- (1) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval.
- (2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim.
- (3) Conspires to commit a violation of subdivision (1), (2), (4), (5), (6), or (7) of this section.
- ...
- (7) Knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the State, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the State.”

600. Pursuant to the North Carolina FCA, based on Defendant's material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. N.C. Gen. Stat. § 1-607(a).

601. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT XXXIX

Unlawful Retaliation Under North Carolina False Claims Act N.C. Gen. Stat. §§ 1-605, et seq.

602. The allegations in the preceding paragraphs are incorporated by reference.

603. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

604. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and efforts to stop Defendant's violations of N.C. Gen. Stat. §§ 1-607, unlawfully retaliated against Relator.

605. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under N.C.G.S.A. § 1-613.

COUNT XL

Rhode Island False Claims Act, R.I. Gen. Laws § 9-1.1-1, et seq.

606. The allegations in the preceding paragraphs are incorporated by reference.

607. Relator also brings this action in the name of the State of Rhode Island, against Defendant pursuant to the State of Rhode Island False Claims Act (“FCA”), R.I. Gen. Laws § 9-1.1-4(b).

608. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the Rhode Island FCA, R.I. Gen. Laws § 9-1.1-3(a), which creates liability for any person who:

- (1) “Knowingly presents, or causes to be presented a false or fraudulent claim for payment or approval;
- (2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;
- (3) Conspires to commit a violation of subdivisions 9-1.1-3(1), (2), (3), (4), (5), (6) or (7); [or]

...

- (7) Knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the state, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the state....”

609. Pursuant to the Rhode Island FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. R.I. Gen. Laws § 9-1.1-3(a).

610. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XLI

Unlawful Retaliation Under Rhode Island State False Claims Act RI Gen. Laws §§ 9-1.1-1, et seq.

611. The allegations in the preceding paragraphs are incorporated by reference.

612. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

613. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and efforts to stop Defendant's violations of RI Gen. Laws §§ 9-1.1-3, unlawfully retaliated against Relator.

614. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under RI Gen. Laws § 9-1.1-4(g).

COUNT XLII

Tennessee False Claims Act, TN Code § 4-18-101 (2015), et seq.

615. The allegations in the preceding paragraphs are incorporated by reference.

616. Relator also brings this action in the name of the State of Tennessee, against Defendant under the Tennessee False Claims Act ("FCA"), TN Code § 4-18-104(c)(1).

617. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the Tennessee FCA, TN Code § 4-18-103(a), which create liability for any person who:

- (1) Knowingly presents or causes to be presented to an officer or employee of the state or of any political subdivision thereof, a false claim for payment or approval;

- (2) Knowingly makes, uses, or causes to be made or used a false record or statement to get a false claim paid or approved by the state or by any political subdivision;
- (3) Conspires to defraud the state or any political subdivision by getting a false claim allowed or paid by the state or by any political subdivision;
- ...
- (7) Knowingly makes, uses, or causes to be made or used a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the state or to any political subdivision;
- (8) Is a beneficiary of an inadvertent submission of a false claim to the state or a political subdivision, subsequently discovers the falsity of the claim, and fails to disclose the false claim to the state or the political subdivision within a reasonable time after discovery of the false claim; or
- (9) Knowingly makes, uses, or causes to be made or used any false or fraudulent conduct, representation, or practice in order to procure anything of value directly or indirectly from the state or any political subdivision.

618. Pursuant to the Tennessee FCA, based on Defendant's material non-

disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State or the political subdivision for treble damages, civil penalties, and all other relief authorized by law. TN Code § 4-18-103(a).

619. As a result of Defendant's violations, the State has suffered damages in an amount to be determined at trial.

COUNT XLIII

Unlawful Retaliation Under Tennessee False Claims Act Tenn. Code Ann. § 4-18-101, et seq.

620. The allegations in the preceding paragraphs are incorporated by reference.

621. During and by virtue of Relator's employment with Salesforce, Relator obtained direct and independent knowledge of Defendant's unlawful conduct alleged in this Complaint.

622. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action, unlawfully retaliated against Relator.

623. As a direct and proximate result of Defendant's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under Tenn. Code Ann. § 4-18-105.

COUNT XLIV

Vermont False Claims Act, 32 V.S.A. § 630-632, et seq.

624. The allegations in the preceding paragraphs are incorporated by reference.

625. Relator also brings this action in the name of the State of Vermont, against Defendant under the State of Vermont False Claims Act (“FCA”), 32 V.S.A. § 632(b).

626. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the Vermont FCA, 32 V.S.A. § 631, which states that no person shall:

- “(1) knowingly present, or cause to be presented, a false or fraudulent claim for payment or approval;
- (2) knowingly make, use, or cause to be made or used, a false record or statement material to a false or fraudulent claim;
- ...
- (8) enter into a written agreement or contract with an official of the State or its agent knowing the information contained therein is false;
- (9) knowingly make, use or cause to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the State; [or]

(10) knowingly conceal or knowingly and improperly avoid or decrease an obligation to pay or transmit money or property to the State;”

627. Pursuant to the Vermont FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the State for treble damages, civil penalties, and all other relief authorized by law. 32 V.S.A. § 631(b).

628. As a result of Defendant’s violations, the State has suffered damages in an amount to be determined at trial.

COUNT XLV

Unlawful Retaliation Under Vermont False Claims Act 32 V.S.A. §§ 630-642

629. The allegations in the preceding paragraphs are incorporated by reference.

630. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

631. Salesforce, with actual knowledge of Relator’s lawful acts in furtherance of this action and efforts to stop Defendant’s violations of 32 V.S.A. § 631, unlawfully retaliated against Relator.

632. As a direct and proximate result of Salesforce’s retaliatory actions, Relator suffered damages and is entitled to all allowable relief under 32 V.S.A. § 638.

COUNT XLVI

The Virginia Fraud Against Taxpayers Act, Va. Code Ann. § 8.01-216.1, et seq.

633. The allegations in the preceding paragraphs are incorporated by reference.

634. Relator also brings this action on behalf of the Commonwealth of Virginia, against Defendant under the Virginia Fraud Against Taxpayers Act (“FCA”), Va. Code Ann. § 8.01-216.5(A).

635. Defendant, through its material non-disclosures and other wrongful acts and omissions set forth above, violated each of the following provisions of the Virginia FCA, Va. Code Ann. § 8.01-216.3(A), which create liability for any person who:

“1. Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;

Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;

Conspires to commit a violation of subdivision 1, 2, 4, 5, 6, or 7;

...

7. Knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Commonwealth or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Commonwealth.”

636. Pursuant to the Virginia FCA, based on Defendant’s material non-disclosures and other wrongful acts and omissions set forth above, Defendant is liable to the Commonwealth for treble damages, civil penalties, and all other relief authorized by law. Va. Code Ann. § 8.01-216.3(A).

637. As a result of Defendant’s violations, the Commonwealth has suffered damages in an amount to be determined at trial.

COUNT XLVII

Unlawful Retaliation Under Virginia Fraud Against Taxpayers Act VA Code Ann. §§ 8.01-216.1, et seq.

638. The allegations in the preceding paragraphs are incorporated by reference.

639. During and by virtue of Relator’s employment with Salesforce, Relator obtained direct and independent knowledge of Defendant’s unlawful conduct alleged in this Complaint.

640. Salesforce, with actual knowledge of Relator's lawful acts in furtherance of this action and efforts to stop Defendant's violations of VA Code Ann. § 8.01-216.3, unlawfully retaliated against Relator.

641. As a direct and proximate result of Salesforce's retaliatory actions, Relator suffered damages and is entitled to all allowable relief under VA Code Ann. § 8.01-216.8.

WHEREFORE, Relator, on behalf of Relator and the United States, prays:

- (a) That the Court enter judgment against Defendant in an amount equal to three times the amount of damages the United States has sustained because of Defendant's actions, plus a civil penalty of any amount within the applicable statutory ranges, for each violation;
- (b) That Relator be awarded an amount that the Court decides is reasonable for recovering the proceeds of the action, including but not necessarily limited to the civil penalties and damages, on behalf of the United States, which, pursuant to the False Claims Act, shall be at least 15 percent but not more than 25 percent of the proceeds of the action or settlement of the claim if the government intervenes and proceeds with the action, and not less than 25 percent nor more than 30 percent of the proceeds of the action or settlement of the claim if the government does not intervene;

- (c) That Relator receives all relief necessary to make Relator whole for Defendant's violations of 31 U.S.C. § 3730(h);
- (d) That the Court order Defendant to awards Relator front pay in lieu of reinstatement;
- (e) That Relator receives an award of two times back pay, including the value of lost benefits and equity;
- (f) That Relator receives an award of compensatory damages in an amount to be proven at trial for the economic, reputational, and emotional harm Relator experienced as a result of Defendant's unlawful conduct;
- (g) That Relator receives an award of punitive damages in an amount sufficient to punish Defendant for its willful and malicious conduct and deter future, similar violations;
- (h) That judgment be entered against Defendant, in the amounts to be determined at trial; and
- (i) That Relator be awarded all costs and expenses incurred, including reasonable attorneys' fees; and
- (j) That the Court order such other relief as is appropriate.

Trial by jury is hereby requested.

Dated: September 8, 2022

Respectfully submitted,





RYAN F. KENNY

M.A. Bar No. 668572

HKM Employment Attorneys LLP

10 High Street, Suite 401

Boston, MA 02110

(617) 297-2002

(206) 260-3055 (fax)

rkenny@hkm.com

JASON RITTEREISER

(pro hac vice pending)

W.A. Bar No. 43628

HUGH BARBER

(pro hac vice pending)

W.A. Bar No. 20420

HKM Employment Attorneys LLP

600 Stewart Street, Suite 901

Seattle, WA 98136

jrittereiser@hkm.com

hbarber@hkm.com

RENÉE BROOKER

(pro hac vice pending)

D.C. Bar No. 430159

EVA GUNASEKERA

(pro hac vice pending)

D.C. Bar No. 502542

JACLYN TAYABJI

D.C. Bar No. 1766350

(pro hac vice pending)

Tycko & Zavareei LLP

1828 L Street NW

Suite 1000

Washington, DC 20036

(202) 417-3664

(202) 973-0950 (fax)

reneebrooker@tzlegal.com

eva@tzlegal.com

jtayabji@tzlegal.com